ДЕПАРТАМЕНТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
ТЮМЕНСКОЙ ОБЛАСТИ

ЦИП центр информационных проектов

Методическое пособие для организации работы по профилактике кибермошенничества на территории Тюменской области

Методическое пособие разработано АНО «Центр информационных проектов» (подведомственная организация Департамента общественных связей Тюменской области) совместно с Прокуратурой Тюменской области, УМВД России по Тюменской области и Отделением Банка России по Тюменской области

Тюмень, 2025

Содержание

1. Введение

Данный документ представляет собой текстовую и аналитическую базу, предназначенную для использования в работе по профилактике кибер- и телефонного мошенничества. Он содержит структурированную информацию, фактуру, формулировки и статистику, которые могут служить основой для подготовки:

- информационных материалов для населения
- контента для сайта и соцсетей
- листовок, памяток, презентаций
- сценариев для видеороликов
- тв- и радиорекламы и др.

Документ предназначен для сотрудников, занимающихся профилактикой кибер- и телефонного мошенничества, и помогает быстро сориентироваться в теме, использовать готовые формулировки.

Зачем нужна эта методичка:

Цель — дать четкие, практические рекомендации по организации информационно-просветительской работы с населением. Вы узнаете, **какие виды мошенничества наиболее распространены**, **как их распознать**, **что и как говорить людям**, и **какие инструменты использовать** в работе.

Что вы найдете внутри:

- Актуальную статистику и проблематику
- Портрет целевой аудитории (кто чаще всего становится жертвой)
- Типичные схемы мошенничества
- Коммуникационные посылы и примеры формулировок
- Практические советы по технологической защите
- Контакты и алгоритм действий, если человек стал жертвой
- Официальные источники информации

2. Краткое содержание методического пособия

1. Сущность и масштаб проблемы

- **Масштаб проблемы**: Кибермошенничество — быстрорастущий вид преступности. В 2024 году россияне **по данным банковской отчетности** потеряли **от действий мошенников** 27,5 млрд рублей, что на **74%** больше, чем в 2023 году. За 1 кв. 2025 года – 6,9 млрд рублей.

- **Региональное влияние**: В Тюменской области в 2024 году число киберпреступлений выросло на 11%, что привело к значительным экономическим потерям и социальной напряженности.

- По данным УМВД Тюменской области – За первое полугодие 2025 года в Тюменской области зарегистрировано более 6 тыс. преступлений, из них 3 875 — мошенничества и кражи с использованием телекоммуникационных технологий, что на 631 больше, чем годом ранее. Ущерб превысил 1,6 млрд рублей (в 2024 году — 2,5 млрд).

- **Уязвимые группы**: Жертвой может стать любой человек, но основными мишенями являются:
    - **Молодежь (14–24 года)**: часто вовлекается в мошеннические схемы в качестве «дропперов» или «помощников» за быстрые деньги.
    - **Работающие граждане (25-44)**: люди со стабильным доходом и средним образованием — частые цели.
    - **Пожилые люди (50+)**: более уязвимы из-за низкой цифровой грамотности.

2. Распространенные схемы мошенничества

- **Телефонные/СМС-мошенничества**: преступники представляются сотрудниками коммунальных служб, поликлиник и других организаций. Преступник создает впечатление, что заботится о вас: записывает к врачу, предлагает заменить счётчики или получить услуги.
- **Фальшивые сайты и приложения**: копируют легитимные платформы для кражи учетных данных или средств.
- **Атаки на аккаунты Госуслуг**: получение доступа к личным кабинетам для оформления микрозаймов.

- **Финансовые посредники**: убеждают людей переводить или отмывать деньги, подвергая их юридическим рискам.

Мошенники часто **воздействуют на эмоции и чувства** людей, чтобы добиться своего — они используют как **положительные**, так и **отрицательные эмоции**. В первом случае жертву вводят в состояние **радости**, **надежды** или **доверия**, сообщая, например: *«Вы выиграли крупную сумму денег»*, *«Вам положены социальные выплаты»* или *«Пенсионный фонд рад сообщить о перерасчете вашей пенсии…»*.

Во втором случае мошенники вызывают **страх**, **панику** или **стыд**, пугая сообщениями вроде: *«С вашего счета списали все деньги»*, *«Ваш родственник попал в аварию и сбил человека»* или *«Беспокоит следователь МВД. Вы являетесь свидетелем по уголовному делу»*. **Понимание этих приемов** поможет **вовремя распознать обман** и **не поддаться на провокацию**.

3. Способы защиты:

- Не берите трубку и не разговаривайте с незнакомцами.
- Установите определитель номера и антивирус на телефон и компьютер.
- Установите двойную защиту аккаунтов и профилей в соцсетях, мессенджерах, почтах и пр. сервисах.
- Запретите оформление кредита на свое имя через Госуслуги.
- Не сообщайте коды из СМС и приложений, данные карт и пароли.
- Игнорируйте подозрительные ссылки и вложения — даже если они пришли от «знакомого».

4. Что делать, если вы стали жертвой мошенника

- **Прекратите контакт**: немедленно завершите общение с мошенником.
- **Свяжитесь с банком**: позвоните в банк для блокировки карты или транзакций.
- **Сообщите в полицию**: подайте заявление с указанием деталей (номера телефонов, скриншоты) через отделение УМВД или Госуслуги.

- **Предупредите других**: сообщите семье/друзьям, чтобы предотвратить дальнейшие атаки.

5. Юридическая защита

- **Ключевые законы**:
  - **Уголовный кодекс (статьи 159, 187)**: предусматривает наказание за мошенничество и незаконные платежные методы, с санкциями до 10 лет лишения свободы.
  - **Гражданский кодекс (статья 179)**: позволяет жертвам аннулировать договоры, заключенные обманным путем.
  - **Федеральный закон № 152-ФЗ**: защищает персональные данные от неправомерного использования.
  - **Федеральный закон № 115-ФЗ**: оказывает противодействие отмыванию денег через мониторинг транзакций.

- **Новые меры (2024–2025)**:
  - Банки обязаны замораживать подозрительные транзакции.
  - Задержка SMS-кодов до завершения звонков.
  - Ограничения на передачу SIM-карт не родственникам.
  - Самозапрет на кредит.

6. Официальные источники информации:

- **Центральный банк России**: cbr.ru/information_security/pmp/
- **Народный фронт «Мошеловка»**: moshelovka.onf.ru
- **Прокуратура Тюменской области** epp.genproc.gov.ru/web/proc_72
- **УМВД России по Тюменской области** 72.mvd.ru
- **Информационный портал «Финансовая культура» Банка России** fincult.info
- **Проект Правительства Тюменской области,** при поддержке Прокуратуры Тюменской области, Управления МВД России по Тюменской области и Отделения банка России по Тюменской области стопмошенники72.рф
- **Детская безопасность в сети. Проект Департамента информатизации Тюменской области** kiber.admtyumen.ru
- **Сбер – раздел «Кибербезопасность»** https://www.sberbank.ru/ru/person/kibrary

3. Актуальность и проблематика

Кибер- и телефонное мошенничество сегодня — **одна из самых массовых и быстроразвивающихся форм преступности.** Мошенники ежедневно совершают миллионы попыток обмана граждан: звонят от имени банков, госорганов, родственников, пишут в мессенджерах, создают поддельные сайты и онлайн-сервисы.

С каждым годом схемы становятся всё сложнее и реалистичнее, а целевая аудитория — шире. От обмана не застрахован никто: жертвами становятся и молодёжь, и пожилые, и люди с высоким уровнем цифровой грамотности.

Информационная профилактика — единственный эффективный способ массовой защиты населения. Люди должны вовремя получать понятные и точные сигналы: как работает обман, как его распознать и что делать, если контакт уже произошел.

Проблематика

Последствия для региона и граждан:

- **Экономический ущерб**: только по официальной статистике ежегодно граждане теряют миллиарды рублей, при этом вернуть средства удается лишь в редких случаях.

- **Социальная напряженность**: потеря денег вызывает стресс, недоверие к банкам и государственным структурам.

- **Рост цифровой уязвимости**: чем выше проникновение цифровых сервисов, тем выше и риски — особенно среди пожилых и уязвимых групп населения.

- **Имиджевые риски**: слабая работа по профилактике создает ощущение безнаказанности мошенников и подрывает доверие к власти.

4. Цели и задачи профилактики мошенничества

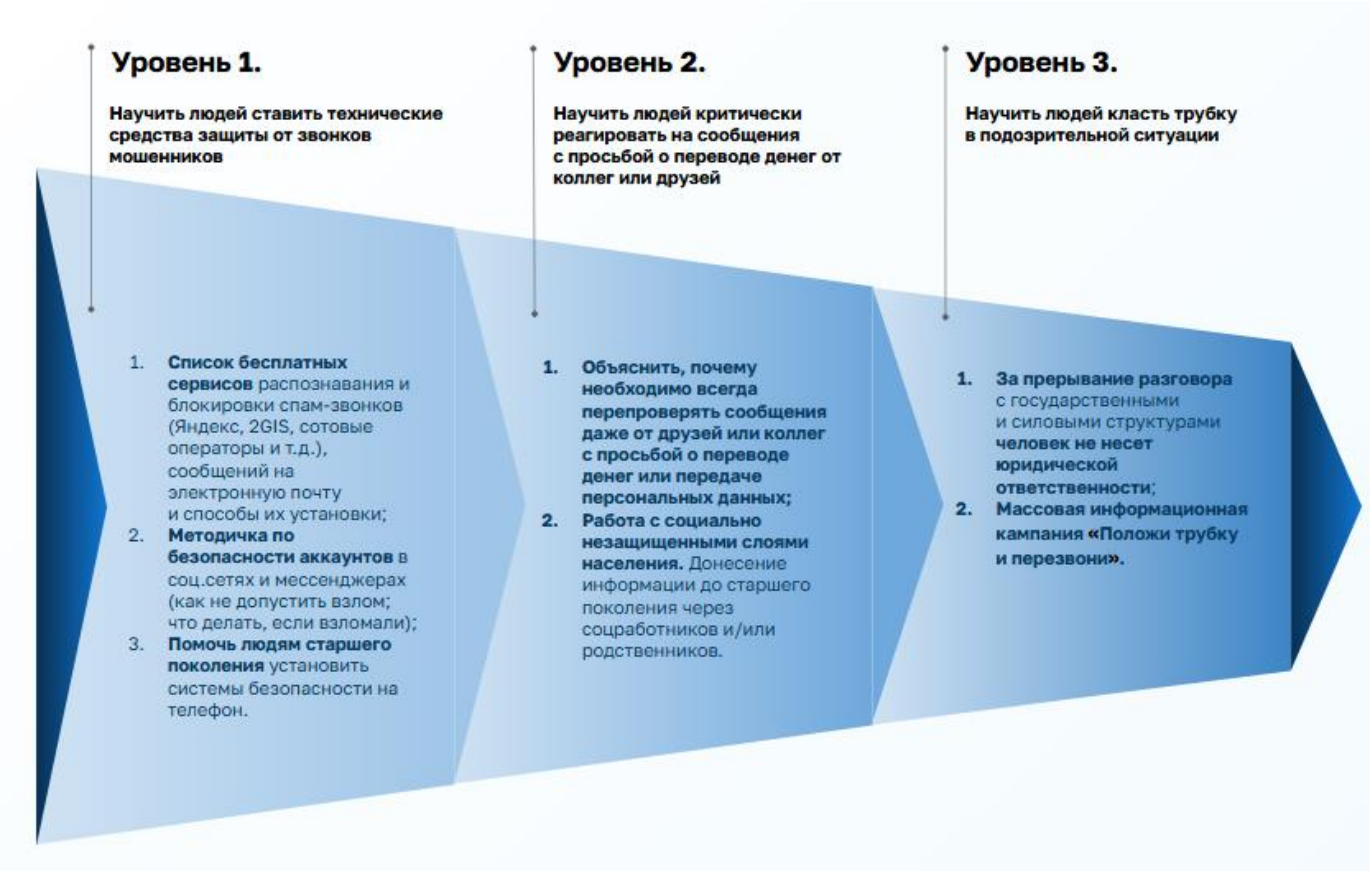
Стратегия профилактики строится на **трех уровнях** *(подробнее на схеме ниже)*, каждый из которых направлен на формирование устойчивого цифрового поведения у жителей региона:

1. **Техническая защита**
   — Научить людей пользоваться бесплатными сервисами защиты: блокировщиками спам-звонков, антивирусами, средствами защиты аккаунтов в соцсетях и мессенджерах.
   — Помочь (особенно людям старшего поколения) установить эти средства на свои устройства.

2. **Критическое восприятие информации**
   — Формировать привычку **перепроверять любые просьбы** о переводе денег, даже от знакомых.
   — Объяснять, как работают схемы с фальшивыми сообщениями от друзей/родственников.
   — Обучать социально уязвимые группы (пенсионеры, малозащищенные) через социальных работников и семью.

3. **Правильная реакция в момент опасности**
   — Закрепить поведение: **не вступать в диалог с мошенниками, сразу класть трубку, не отвечать.**
   — Единый слоган «Не разговаривай с незнакомцами» направлен на то, чтобы это правило стало нормой.

Стратегия профилактики мошенничества



Реализация профилактики

Для достижения целей проекта используется **механика** *(подробнее на схеме ниже)*, включающая:

- **Единая информационная платформа**
  — сайт **стопмошенники72.рф**

  — Детская безопасность в интернете **kiber.admtyumen.ru**

  где собраны обучающие материалы, инструкции, видеоконтент, тесты и ссылки

- **Вовлечение населения через обучение**
  — тренинги для сотрудников органов власти и подведомственных учреждений и обучение групп риска - дети и пенсионеры.
  — обучение целевых групп риска — молодежь, средний возраст, пенсионеры *(см. подробнее след. раздел)*
  — мероприятия для населения с охватом до 200 000 человек.

5. Портрет жертвы (Целевая аудитория)

Кто чаще становится жертвой:

1. Молодёжь (14–24 года)

Молодые люди часто вовлекаются в сомнительные схемы как дропперы или «помощники». Им предлагают лёгкие деньги за переводы или оформление карт. Недостаток жизненного опыта и стремление к заработку делают подростков уязвимыми, особенно через соцсети и мессенджеры.

---

2. Средний возраст (25–44 года)

По данным Банка России, основная группа риска — это экономически активные граждане.
Люди в возрасте от 25 до 44 лет — частые пользователи интернет-банков, маркетплейсов, служб доставки, мессенджеров. Мошенники используют привычные сценарии: *“с вашей карты списание”, “злоумышленники в Сбербанке”, “безопасный счёт”, “блокировка аккаунта”*. Уверенность в своей цифровой грамотности часто мешает людям вовремя заметить обман.

---

3. Пенсионеры (60+)

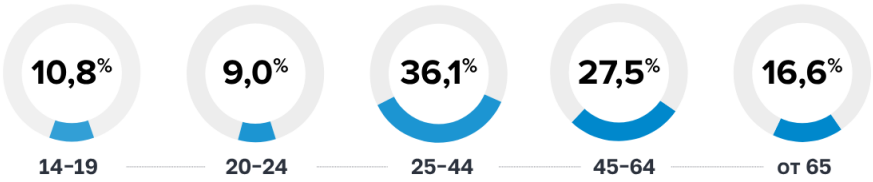
Пожилые люди — также одна из самых уязвимых категорий. Они доверчивы, чувствительны к тревожным сообщениям, не умеют критически мыслить и считают невежливым прерывать разговор.

Им звонят от “внука”, “врача”, “полиции” или “банка”, используют поддельные номера и голоса. Особенно уязвимы для голосовых и визуальных манипуляций (глубоких фейков).

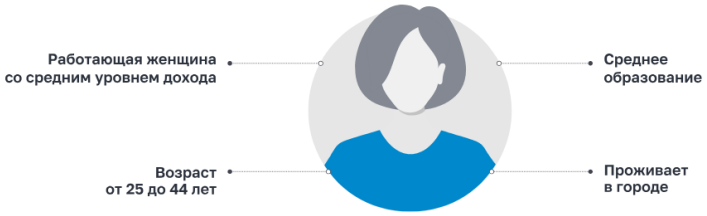
Ниже представлен обобщенный портрет пострадавшего от кибермошенничества, составленный на основе данных ежегодного опроса Банка России за 2024 год. *Отчет доступен по ссылке.*

Кто чаще всего попадается на уловки мошенников

Стать жертвой кибермошенников может любой человек. Тем не менее наибольший интерес для них представляют граждане, которые проявляют высокую экономическую активность и часто пользуются банковскими сервисами – люди в возрасте от 25 до 64 лет. Среди пострадавших наблюдается рост числа граждан старше 65 лет.

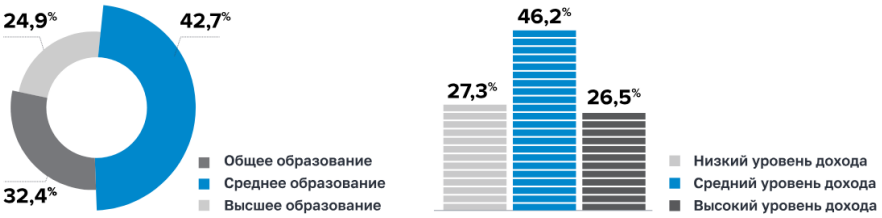


В 2024 году жертвами мошенников чаще всего становились работающие женщины со средним уровнем дохода и средним образованием, которые проживают в городе и имеют постоянную занятость.



Если в 2023 году среди пострадавших доля женщин была существенно (на 11 п.п.) выше доли мужчин, то в 2024 году этот разрыв сократился (на 5,2 п.п.). Активность мошенников против жителей сельских территорий незначительно выросла.

Уровень образования и достатка



6. Ключевые посылы и коммуникационные тезисы

Основная идея кампании — сформировать у людей **единственно правильную модель поведения** при столкновении с мошенничеством: **не вступать в контакт, не вести диалог, не реагировать**.

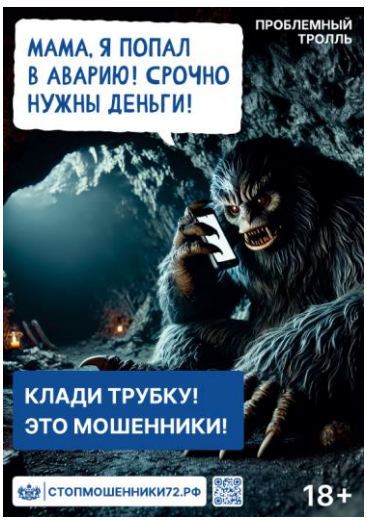
Ключевой слоган кампании: **«Клади трубку! Это мошенники!»**

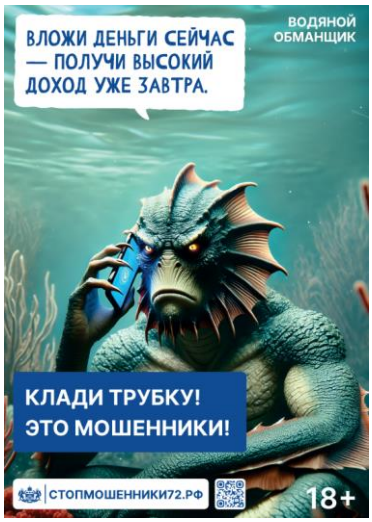
Это не просто лозунг, а **четкое правило**, которое должен запомнить каждый: если не уверен в источнике — не отвечай, не продолжай разговор, не доверяй.

Кампания основана на визуальной и эмоциональной аллегории: **мошенник — это монстр**, незаметный, но опасный, способный «похитить» деньги, данные и спокойствие. Его нужно не разоблачать, а **игнорировать и прерывать контакт** на начальном этапе.

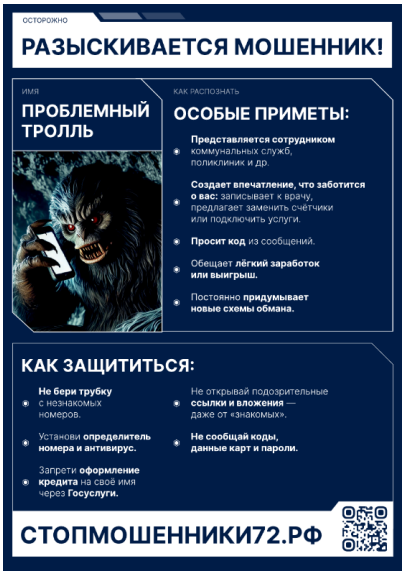
Визуальные концепции, поддерживающие посылы:

1. **Мифические монстры** — образ мошенников как неведомой опасности. Работает на запоминание и эмоции.






ЛЕТАЮЩИЙ КОДОПРОС
ПРОЙДИТЕ МЕДОСМОТР. ДЛЯ ЗАПИСИ НАЗОВИТЕ КОД ИЗ СМС.
КЛАДИ ТРУБКУ! ЭТО МОШЕННИКИ!
СТОПМОШЕННИКИ72.РФ
18+
ОГНЕННЫЙ ЛЖЕЦ
ВЫ ПЕРЕВЕЛИ ДЕНЬГИ УКРАИНСКИМ ВОЙСКАМ. НА ВАС ЗАВЕДЕНО УГОЛОВНОЕ ДЕЛО.
КЛАДИ ТРУБКУ! ЭТО МОШЕННИКИ!
СТОПМОШЕННИКИ72.РФ
18+


ОСТОРОЖНО
РАЗЫСКИВАЕТСЯ МОШЕННИК!
ИМЯ
ПРОБЛЕМНЫЙ ТРОЛЛЬ
КАК РАСПОЗНАТЬ
ОСОБЫЕ ПРИМЕТЫ:
Представляется сотрудником коммунальных служб, поликлиник и др.
Создает впечатление, что заботится о вас: записывает к врачу, предлагает заменить счётчики или подключить услуги.
Просит код из сообщений.
Обещает лёгкий заработок или выигрыш.
Постоянно придумывает новые схемы обмана.
КАК ЗАЩИТИТЬСЯ:
Не бери трубку с незнакомых номеров.
Установи определитель номера и антивирус.
Запрети оформление кредита на своё имя через Госуслуги.
Не открывай подозрительные ссылки и вложения — даже от «знакомых».
Не сообщай коды, данные карт и пароли.
СТОПМОШЕННИКИ72.РФ

7. Основные схемы мошенничества

Мошенники используют разнообразные схемы обмана, которые постоянно адаптируются к цифровым привычкам граждан.

Мошенники используют разнообразные схемы обмана, которые постоянно адаптируются **под актуальную новостную повестку** и к цифровым привычкам граждан.

Следует помнить, что атаки становятся персонифицированными, тщательно подготовленными. Злоумышленники стали предварительно изучать жертву: ее профиль в социальных сетях, круг друзей, увлечения, место работы.

Ниже — наиболее распространенные сценарии, актуальные для Тюменской области и всей России:

Легенда звонка	Цель мошенника	Приемы и технологии
«Звонок из управляющей компании / энергосбыта / водоканала» Вам звонит человек, представляющийся **сотрудником коммунальных служб, поликлиники или иной официальной организации**.	Получить данные банковской карты, персональные сведения или заставить перевести деньги «на счёт организации» под видом оплаты услуг или долгов.	Сообщает о **задолженности** или «необходимости срочной замены оборудования» (счётчиков, кабеля и т. п.). Может предложить **записать на прием к врачу** или «получить льготу/услугу». Создает **ощущение срочности и заботы**: «чтобы не было отключения», «чтобы не потерять льготу», «для вашего удобства». Может **знать адрес, ФИО** и другие персональные данные. Использует **подмену номера**, звонок отображается как из «УК», «ЕИРЦ», «Поликлиника». Может «переключить» на другого «специалиста». Итог: человек **сам переводит деньги**

		мошенникам или передаёт конфиденциальные данные.
«Инвестиции с доходом 30–100%» «Вы оставляли заявку на платформе — хотим предложить вам вложение под высокий доход»	Вовлечь в псевдоинвестиции и вывести ваши деньги. Жертве обещают высокую доходность от вложений — в криптовалюту, «новые технологии», «госпрограммы». Человека убеждают перевести деньги, установить инвестиционное приложение или передать доступ к устройству (через AnyDesk и аналоги).	– «Аналитик» помогает зарегистрироваться на фейковом сайте. – Вас просят вложить сначала 5 000 ₽, затем больше. – После каждого пополнения «баланс растет» , но вывести средства невозможно. – Итог: деньги пропадают, платформа исчезает, сотрудники не выходят на связь.
«Звонок пенсионерам на стационарный телефон» Пожилым людям звонят на домашний телефон, представляясь сотрудниками **коммунальных служб, поликлиники, «Горводоканала», социальных или государственных ведомств**.	Сначала — выманить у пенсионера собственные деньги под видом оплаты услуг или «во избежание отключения». Далее — вовлечь пожилого человека в схему: использовать его как **курьера («дропа»)** для сбора денег у других жертв.	Разговор строится так, будто звонящий заботится о человеке: напоминает о долгах, предлагает услуги или помощь. После этого подключаются «другие службы» — пенсионеру звонят повторно уже от имени других организаций, постепенно втираясь в доверие. После нескольких таких звонков пенсионеров могут уговаривать **передать деньги курьеру**. Следующий шаг — вовлечение самих пенсионеров в схему: их просят **забирать деньги у других пожилых людей** и привозить «в организацию». Таким образом жертва превращается в **«дропа» или курьера**, участвует в цепочке мошенников, часто не понимая своей роли.
«Вы совершили преступление, спонсируете ВСУ»	«Вы попали в базу, с вашей карты отправлялись деньги на финансирование ВСУ. Чтобы не было уголовного	– Представляются сотрудниками МВД, Центробанка, ФСБ. Часто звонят с подменного номера. – Просят не рассказывать

	дела, нужно сотрудничать с безопасностью». Запугать жертву обвинением в преступлении и выманить деньги «для проверки», «для безопасности» или якобы «чтобы доказать невиновность». Жертву вводят в стресс: говорят, что с её карты якобы шли переводы на финансирование террористов, открыто уголовное дело, скоро приедет полиция. Предлагают "разобраться" — и втягивают в цепочку ложных процедур.	никому, говорят, что идет «секретное расследование». – Убеждают перевести деньги «на безопасный счёт», чтобы доказать, что вы не преступник. – Могут просить установить удалённый доступ (AnyDesk и аналоги), чтобы «помочь» или «зафиксировать доказательства». – Итог: вы передаёте свои деньги мошенникам, а потом они исчезают.
«Пенсионный фонд / Соцвыплаты» **«**Вам положена доплата, перерасчет пенсии или возврат взносов**»** — так начинается разговор.	Выманить персональные и банковские данные или получить плату за перевод компенсации».	– Спрашивают паспортные данные, СНИЛС, реквизиты карты. – Под предлогом «идентификации» просят фото карты, CVV-код. – Могут сообщить о «комиссии» за перевод и предложить перевести деньги. – Итог: хищение средств или оформление кредита на вас.
«Вас приглашают на диспансеризацию / медосмотр на дому» Вам звонят якобы из поликлиники или частной клиники и предлагают пройти бесплатный медосмотр, вакцинацию, диагностику на дому.	Попасть в квартиру для кражи или навязать платные услуги.	– «Врач» или «фельдшер» приходит с сумкой, показывает липовые документы. – Втирается в доверие, пока вы отходите или приносите документы — крадет вещи. – Иногда оставляют липовые «счета» за осмотр. – Итог: хищение наличных, ценностей или выманивание подписей на кредит.
«Ваш родственник попал в ДТП» Звонок ночью или рано утром: **«**Ваш сын попал в	Испугать и заставить быстро перевести деньги.	– На фоне — крики, плач, имитация паники. – Иногда используют дипфейк-голос: «Мам, это я, помоги!»

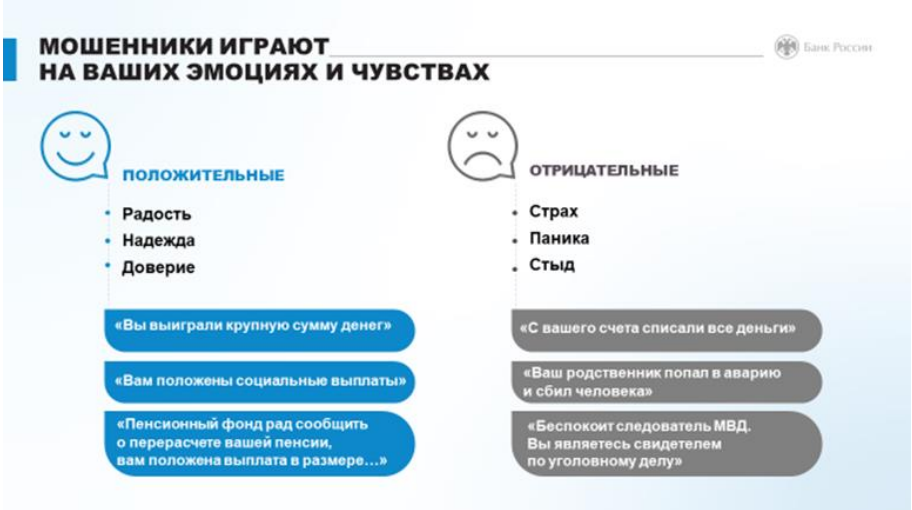
аварию, чтобы его не посадили, нужно срочно перевести деньги»		– После вступает «следователь», «адвокат», просит перевести деньги. – Итог: деньги переведены мошенникам, родственник на самом деле в порядке.
«Звонок сотрудника Центрального банка» Вам сообщают, что по карте зафиксирована подозрительная активность - деньги пытаются перевести со счета (в т.ч. за рубеж). Спасти их можно только одним способом — открыть в Центробанке «защищенный»/»безопасный »/ «специальный» счет.	Убедить человека самостоятельно перевести деньги мошенникам.	– Сначала вас пугают: «Ваш счет скомпрометирован. Деньги вот-вот уйдут.» – Затем предлагают помощь — перевести все на безопасный «временный» счет. – Дается «номер счета» или просят выполнить операции в приложении под диктовку. – Убедительно рассказывают, что это практика «Центрального банка». – Итог: вы сами отправляете свои деньги мошенникам.
«Звонок от сотового оператора» Вам звонят и сообщают о несанкционированной переадресации звонков или проблеме с SIM-картой.	Получить доступ к вашим СМС и звонкам — в том числе кодам из банка или Госуслуг.	— Просят ввести на телефоне специальные команды: *21*номер# или ##002#. – Ложная цель: «отключить подозрительную переадресацию». – После этого мошенник получает управление вашими звонками. – Возможно: подсовывают поддельную ссылку на «перепривязку» сим-карты. – Итог: коды подтверждения приходят не вам, а мошеннику.
«Звонок от портала Госуслуг / суда» Вам сообщают, что на ваше имя подан иск или что есть проблемы с учетной записью.	Получить СМС-код и захватить ваш аккаунт на Госуслугах.	– Говорят, что иск уже в работе, но документы можно посмотреть только через Госуслуги. – Присылают ссылку на поддельный сайт, где просят ввести логин и СМС-код. – Иногда отправляют QR-код для «быстрого входа». – Итог: доступ к Госуслугам перехвачен, далее —

		оформление займов, взлом банков, доступ к документам.
«Помощник судьи / судебный пристав» «Против вас идет гражданское дело. Требуется подтверждение личности для доступа к материалам»	Захват доступа к Госуслугам или Сбер ID.	– Присылают ссылку на «портал суда» (поддельный). – Вы вводите логин, пароль и СМС. – Могут попросить вас пройти «удаленную идентификацию» — включить экран или установить программу. – Итог: доступ ко всем государственным и банковским сервисам.
«Обновление банковского приложения» «Приложение устарело, сейчас вышло обновление. Чтобы не потерять доступ, нужно установить вручную»	Заставить установить вредоносное приложение.	– Скидывают ссылку на установочный файл (apk-файл). – Программа дает мошеннику доступ к экрану, звонкам, клавиатуре. – После установки вас «проводят» по интерфейсу — вы сами вводите все нужное. – Итог: вы теряете контроль над устройством, мошенники списывают деньги.
«Звонок из налоговой службы» «У вас задолженность по налогу на землю/машину. Сегодня крайний срок, иначе штраф и арест»	Получить деньги или доступ к карте.	– Говорят официальным тоном, называют фейковый ИНН. – Присылают поддельную квитанцию или ссылку на оплату. – Итог: деньги уходят мошенникам, в базе ФНС никаких долгов нет.
«Оплатил товар — где заказ?»	«Я перевёл деньги, вот чек. Почему вы не отправляете товар?» Вовлечь предпринимателя в фиктивную сделку и обманом выманить деньги, товар или персональные данные.	– Присылают поддельные скриншоты «успешной оплаты» с фейкового интернет-банка. – Зачастую намеренно указывают сумму больше нужной и просят вернуть «ошибочно лишнее». – Могут торопить: «Отправьте прямо сейчас, мне срочно», чтобы продавец

	Мошенник притворяется покупателем: оформляет заказ, присылает поддельный платёжный чек, торопит с отправкой. Может попросить «вернуть переплату» или выведать реквизиты для перевода — чтобы использовать их в других схемах.	не успел проверить поступление. – Иногда оформляют доставку через курьера, чтобы получить товар, не оплатив. – Итог: товара нет, деньги не пришли, «покупатель» исчезает.
«Это я — срочно нужна помощь» **«Мама/бабушка, срочно переведи деньги»**	«Привет! Я попал в беду, срочно переведи деньги — потом всё объясню». Используют поддельный голос или видео, чтобы ввести в заблуждение и выманить деньги. Мошенники используют нейросети, чтобы сгенерировать голос, похожий на голос родственника, друга или коллеги. Иногда — видео с их лицом. Просят деньги «на лечение», «штраф», «аванс» и т.д.	– Используют аудио или видео, сгенерированные на основе открытых данных (соцсети, YouTube и др.). – Пишут или звонят в мессенджерах: WhatsApp, Telegram — голосовое сообщение или видеозвонок. – В сообщениях создают панику: авария, задержание, срочная операция. – Давят на эмоции: «Не звони никому, мне стыдно», «только ты можешь помочь». – Итог: жертва переводит деньги мошенникам, думая, что спасает близкого.
«Звонок из службы безопасности банка» Вам звонит человек, представляющийся сотрудником службы безопасности банка. Он говорит, что на вашем счете зафиксирована подозрительная операция (перевод, покупка, снятие наличных), и необходимо срочно принять меры.	Выманить ваши деньги под предлогом «спасения» или получить доступ к онлайн-банку.	– Мошенник утверждает, что «внутри банка» работает группа преступников, и деньги необходимо перевести на якобы безопасный счет Центробанка. – Может переключить вас на «старшего специалиста» или «представителя ЦБ». – Может попросить установить программу для удаленного доступа, чтобы «помочь». – Заставляет вас не рассказывать о происходящем никому — «это тайная операция». – Использует подмену номера: звонок якобы с номера банка.

		– Итог: вы сами переводите деньги на счет мошенников.

Приемы воздействия мошенников



8. Как гражданин может быть втянут в преступление

Мошенники часто используют доверчивых людей, **людей в сложном финансовом положении в роли дропов - посредников злоумышленников для перевода и обналичивания похищенных денег.**

Чем занимаются дропперы:
– получают на свои карты деньги и передают их дальше по цепочке другим людям – наличными или переводом;
– принимают наличные деньги, вносят их на свои счета для последующего перевода или передают другим людям;
– предоставляют мошенникам в пользование свои карты или доступ к онлайн-банку.

Ниже — реальные сценарии, чем это может обернуться и почему важно отказываться от подобных предложений.

1. Просьба перевести деньги через ваш счёт или карту

Как выглядит:

- «Я по ошибке перевел вам деньги – верните, пожалуйста»,
- «Помоги перевести деньги — у меня проблемы с банком»,
- «На мой счёт нельзя принимать переводы — можешь переслать деньги дальше?»
- «Ты же не против получить на карту 1000 ₽ и перекинуть 900 ₽ мне?»

Что происходит на самом деле:
Мошенники используют ваш счет как промежуточное звено для отмывания украденных денег (например, у пенсионеров или жертв фишинга). Это называется "обналичивание через дроппера".

Чем грозит:

- Вы можете стать соучастником хищения средств.
- Вас вызовут на допрос, заблокируют карту, могут временно заморозить счета.

- Даже если вы «не знали», по закону это не освобождает от ответственности — суд оценивает должен ли был человек понимать, что участвует в подозрительной схеме.

2. Удалённая работа «с переводами» или «финансовым помощником»

Как выглядит:

- «Простой доход — принимай переводы и отправляй дальше, всё легально»
- «Ты как будто курьер: деньги пришли — ты переслал»
- «Ты не участвуешь в обмане, просто получаешь процент».

На деле:

Это классическая схема отмывания денег. Вас используют как финансового посредника, через которого проходит украденное. Иногда таких людей нанимают для перевода средств между криптокошельками, картами или в зарубежные банки.

Чем грозит:

- Уголовное преследование, особенно если мошенники обманули десятки людей.
- Конфискация средств, блокировка счетов.
- Запись в базе Росфинмониторинга (что закрывает доступ к банкам, кредитам, иногда — работе).

3. Заведение карты на ваше имя по просьбе «знакомых»

Как выглядит:

- «Помоги — мне не дают открыть карту, а мне очень надо»,
- «Оформи карту/кошелёк — я буду пользоваться, тебе ничего делать не нужно».

Что происходит:

Вы открываете банковский продукт, а им пользуются злоумышленники — для фишинга, обмана, вывода криптовалюты. Документы оформлены на вас — значит, вы отвечаете.

Чем грозит:

- Вы можете оказаться владельцем счета, с которого обманывали других людей.
- Против вас могут возбудить дело за пособничество, особенно если суммы крупные.
- Даже если карта была «подарена» — ответственность несёт владелец.

4. Регистрация на подозрительных сайтах / в приложениях

Как выглядит:
- «Зарегистрируйся и получишь бонус»,
- «Помоги пройти верификацию через Госуслуги»,
- «Введи свои данные — это нужно “для работы”».

На деле:
Через вашу регистрацию мошенники получают доступ к легализованному аккаунту на своё имя — его используют для обмана других людей, взятия микрозаймов, фейковых инвестиций и т. д.

Чем грозит:
- Утечка ваших данных, проблемы с кредитной историей.
- Возможно уголовное или административное разбирательство, если на вашу личность оформлены преступные действия.

Как защитить себя
- Никогда не принимайте чужие переводы без официального подтверждения цели.
- Не открывайте карты или кошельки на третьих лиц, даже если это «друзья».
- Не передавайте доступ к своим аккаунтам (Госуслуги, банк, криптокошелёк).
- Сомневаетесь — консультируйтесь с юристом или банком.

Важно знать:
Помимо блокировки счетов и уголовной ответственности, дропперы сталкиваются с рядом других серьезных последствий:

- они попадают в базу данных Банка России как участники мошеннических операций;
- банки вправе заблокировать им карты и отключить доступ к онлайн-банку (обязательно, если информация о дроппере поступила от полиции);
- не смогут переводить себе или другим больше 100 000 рублей в месяц через карты и онлайн-банк;
- в соответствии с Федеральным законом от 24.06.2025 № 176-ФЗ, с 5 июля 2025 года введена уголовная ответственность за участие в подобных схемах — поправки в статью 187 УК РФ предусматривают лишение свободы на срок от 3 лет.

Даже если вы «не знали», по закону это не освобождает от ответственности — суд оценивает должен ли был человек понимать, что участвует в подозрительной схеме.

9. Статистика

Общероссийская статистика

2024 год:

- Кибермошенничество — быстрорастущий вид преступности. В 2024 году россияне **по данным банковской отчетности** потеряли **от действий мошенников** 27,5 млрд рублей, что на **74%** больше, чем в 2023 году (15,8 млрд). За 1 кв. 2025 года – 6,9 млрд рублей.
- Для масштабности проблемы можно использовать данные МВД России, озвученные в публичном пространстве: В 2024 году ущерб от действий кибермошенников вырос на 36% и составил 200 млрд рублей.

Основные каналы хищений 2024 год:

- **Мобильные приложения банков:**
  Украдено — 9,6 млрд рублей
  Возмещено — 1,3 млрд

- **Социальная инженерия:**
  Вредоносные ссылки, SMS-фишинг.

Центробанк направил информацию о 1 335 фишинговых Интернет-ресурсах с целью их последующей блокировки.

На основании сведений Банка России был ограничен доступ к 44 713 интернет-ресурсам.

- **Телефонное мошенничество:**
  Зафиксировано 1,5 млн попыток обмана (рост +17% к 2023 году)
  Средний ущерб — **57 000 рублей на человека**
  37% пострадавших — люди **старше 55 лет**

Добавлено примечание ([1]): Ссылки на источники

https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516?

https://www.cbr.ru/analytics/ib/operations_survey/2024/

https://cbr.ru/statichtml/file/173923/kgo_2024.pdf

https://www.computerra.ru/314514/banki-predotvratili-hishhenie-4-6-trln-rublej-v-i-kvartale-2025-goda/

https://cisoclub.ru/hakery-vyveli-s-decentralizovannoj-birzhi-gmx-42-mln-dollarov-ispolzovav-ujazvimost-v-pule-likvidnosti/

За I квартал 2025 года:

- Потери от несанкционированных операций — **6,9 млрд рублей** (296,6 тыс. случаев)
- Банки заблокировали **43,8 млн подозрительных транзакций**
- Благодаря этому удалось предотвратить хищения на сумму **4,6 трлн рублей**

Ссылка на исследование от ЦБ России

Ниже данные ежегодного опроса Банка России за 2024 год. Ссылка

Как мошенники пытались получить доступ к деньгам*

Телефонное и СМС-мошенничество до сих пор преобладает, хотя за год доля этого канала обмана сократилась (на 8,4 п.п.). Впервые в пятерке популярных у кибермошенников приемов — получение доступа к аккаунтам людей на Госуслугах.

На остальные каналы мошенничества (фишинговые ресурсы, поддельные QR-коды и прочие) пришлось 13,7%.

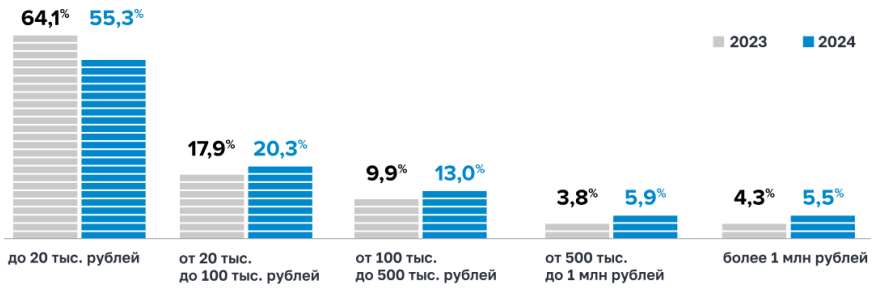
* Учитывались ответы не только пострадавших, но и контактировавших с мошенниками.

Какие действия совершали пострадавшие под влиянием мошенников

Произошел рост числа людей (+3,2 п.п.), которые совершили какое-либо действие под влиянием мошенников.

Сколько денег теряют

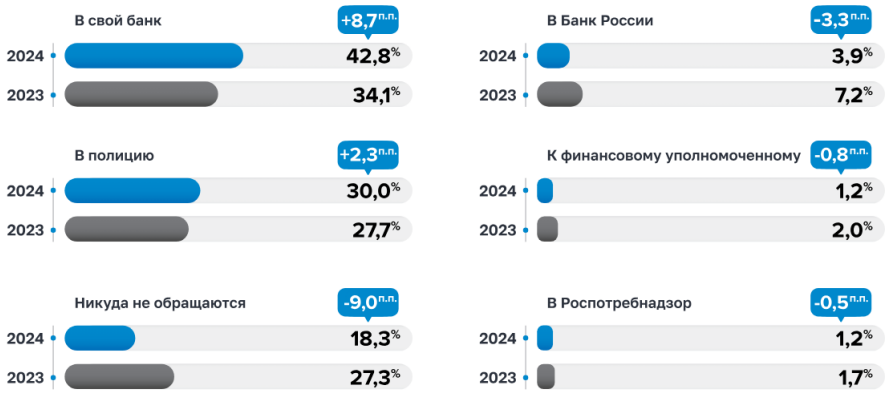
Растет доля хищения сумм свыше 20 тыс. рублей.



В 2024 году респондентам впервые было предложено уточнить, были ли похищенные деньги собственными или кредитными.

Куда обращаются пострадавшие*

Сократилось количество граждан, которые в результате обмана никуда не обращались для защиты своих прав. Среди них в основном пострадавшие, сумма ущерба которых менее 20 тыс. рублей.



* Предлагался множественный выбор ответов.

Статистика в Тюменской области

2024 год:

- По данным прокуратуры, в **2024 году** число киберпреступлений в регионе выросло на **11%** — с 9 540 до **10 625 случаев**.
- Почти **половина всех преступлений** в области — это кибермошенничество (**44,4%** от общего числа).
- **Ущерб** от таких преступлений составил **более 1,4 млрд рублей**.
- **Раскрываемость низкая**: всего **23,9%** дел удалось раскрыть.

За I квартал 2025 года:

- За 3 месяца 2025 года **рост киберпреступности составил 17,6%** (с 2,6 до 3 тыс.), из них на 21,7% возросло число хищений (с 1,6 до 1,9).
- Раскрываемость IT-преступности составила – 22% (32,7%), из них хищений – 11,3% (10,2%).

Данные УМВД от июля 2025:

За 6 месяцев 2025 года на территории Тюменской области зарегистрировано свыше 6 тыс. преступлений, из них по линии мошенничества и краж, с использованием телекоммуникационных технологий 3 875 преступлений, что на 631 преступление больше, чем за аналогичный период прошлого года. Ущерб причиненный жителям нашего региона составил свыше 1 600 000 000 рублей, по итогам 2024 года 2 500 000 000 рублей.

Данные прокуратуры от июля 2025:

За первые шесть месяцев текущего года количество преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на **24,5%** — с **4,9 до 6,1 тысячи** случаев. Их доля в общей структуре преступности составила **46,5%** (в прошлом году — **42%**). Однако раскрываемость таких преступлений остаётся низкой — раскрыто менее трети, всего **19,8%** (ранее — **29,3%**).

Основную часть преступлений составляют **хищения** (по статьям 158–159.6 УК РФ). Их количество выросло на **19,4%** — с **3,2 до 3,9 тысячи** случаев. Это **63%** от всех зарегистрированных преступлений. При этом раскрываемость хищений ещё ниже — всего **8,4%** (в прошлом году — **11,9%**).

Общий **ущерб** от расследуемых преступлений составил **1 млрд 235 млн рублей** (в прошлом году — **892,5 млн**).

Из этой суммы:

- Добровольно возмещено — **14,3 млн руб.** (в прошлом году — **2,9 млн**);
- Через суды (гражданские и арбитражные) взыскано — **9,6 млн руб.**;
- Изъято имущества, денег и ценностей — на сумму **23,3 млн руб.** (в прошлом году — **2,8 млн**).

Данные от Прокуратуры ТО, август 2025:

За 7 месяцев 2025 года зарегистрировано 6,8 тыс. преступлений — на 17,9% больше, чем годом ранее.

Результаты социологического исследования на территории Тюменской области (август, 2025)

- **Количество респондентов:** 553 человека.
- **Пол:** мужчины – 44%, женщины – 56%.
- **Возраст:** 18–24 (9%), 25–34 (16%), 35–44 (23%), 45–54 (16%), 55–64 (16%), 65+ (20%).
- **География:** г. Тюмень – 55%, г. Тобольск – 7%, другие населённые пункты – 38%.

ТОП-5 видов мошенничества, с которыми сталкивались жители:

1. Маскировка под представителей правоохранительных органов – **44%**.
2. Маскировка под операторов сотовой связи – **35%**.
3. Маскировка под представителей финансовых организаций – **34%**.
4. Взлом личных аккаунтов – **29%**.
5. Маскировка под друзей/родственников «в беде» – **18%**.

Только **5%** опрошенных заявили, что **никогда** не сталкивались с телефонным или интернет-мошенничеством.

Основные тезисы:

- 93% сталкивались с мошенничеством (лично или у близких).
- 33% лично верили мошенникам.
- 34% респондентов или их близкие понесли материальный ущерб.
- 71% пытались вернуть похищенные деньги (чаще обращались в полицию – 58%/МВД, 21% – в банк).

- 90% слышали о «самозапрете» на кредиты (26% уже подключили, **23% готовы подключить, 29% не готовы подключить**).
- 72% знают о «дропперстве» (**28% слышат впервые).**

- Самооценка навыков защиты: 4,06 из 5.
- 52% пользуются программами и сервисами для защиты от мошенничества. **34% - нет.**

- Меры предосторожности:

- 88% не передают пароли/коды.
- 71% не хранят данные карт.
- 71% не открывают подозрительные ссылки.

Информированность:

- 72% видели материалы о противодействии мошенничеству (61% в соцсетях, 54% по ТВ, 35% от банков).
- **36% хотели бы получать больше информации.**

Источники, откуда жители хотят получать информацию о кибербезопасности:

- Мессенджеры (Telegram, WhatsApp и др.) – 54%.
- Социальные сети (ВКонтакте, Одноклассники и др.) – 45%.
- Телевидение – 42%.
- Поисковые системы (Яндекс, Google и др.) – 39%.
- Сайты СМИ и новостные порталы – 38%.
- Информация от банка (в приложении, уведомления, на сайте) – 33%.

Ключевые темы, которые интересуют жителей Тюменской области:

1. Как распознать звонки и сообщения мошенников – 53%.
2. Как распознать фейковые сайты, приложения, письма и ссылки – 53%.
3. Как обезопасить пожилых родственников и детей – 49%.
4. Как защитить персональные данные от утечек и кражи – 48%.
5. Как настроить телефон и компьютер для защиты – 42%.
6. Куда обращаться, если стал жертвой мошенничества – 42%.
7. Как проверить, не оформлены ли кредиты на своё имя – 37%.
8. Где найти реальные примеры мошеннических схем – 35%.
9. Как защитить аккаунты от взлома – 31%.
10. Как вести переговоры с мошенниками – 20%.

10. Технологическая защита от мошенничества

Технические инструменты защиты — это первый рубеж обороны, который помогает снизить риск стать жертвой кибермошенников. В этом разделе собраны практические рекомендации по защите **смартфона**, **мессенджеров** и **персонального компьютера** — самых уязвимых каналов, через которые совершаются атаки.

10.1. Технологическая защита смартфона

Смартфон — главный инструмент современного человека, но и один из самых частых каналов атаки.

Рекомендации по защите:

- Установить приложение-блокировщик спам-звонков или определитель номера (**примеры доступны в** **Приложении 1**).
- Использовать **биометрическую защиту**, PIN-коды и двухфакторную аутентификацию.
- **Не устанавливать приложения** из непроверенных источников.
- Отключить автоматическую установку APK-файлов.

- Регулярно обновлять операционную систему и приложения.
- Не передавать SIM-карту, телефон или доступ к ним третьим лицам.

10.2. Технологическая защита мессенджеров

Чтобы защититься от мошеннических звонков в популярных мессенджерах, можно ограничить входящие вызовы с неизвестных номеров.

Рекомендации по защите мессенджеров:

- Включить **двухэтапную авторизацию**.
- Не переходить по ссылкам от незнакомцев, даже если они приходят «от друзей».
- Проверять, не было ли **дубликата** (клона) аккаунта.
- Не отправлять скриншоты с личными данными.
- Ограничить доступ к фото, статусу, номеру телефона для незнакомых пользователей.

Подробная инструкция установки блокировки нежелательных звонков для Telegram и WhatsApp доступна в Приложении 2.

10.3. Технологическая защита персонального компьютера

Фишинговые сайты, поддельные письма, вредоносное ПО — частые угрозы для пользователей ПК.

Рекомендации по защите компьютера:

- Установить и регулярно обновлять антивирус.

- Использовать **надежные браузеры** с включенными функциями защиты от фишинга.

- Проверять адрес сайта перед вводом логинов/паролей (особенно банковских).

- Хранить пароли в **менеджерах паролей**, а не в блокноте или браузере.

- Установить расширения для защиты (например, Web of Trust или AdGuard).

11. Как защитить себя: практические советы

Общие правила безопасности:

1. **Поговорите с членами семьи — особенно с пожилыми и детьми.** Обсудите, как действовать в случае подозрительных звонков или сообщений. **Рассказывайте близким о типичных схемах мошенничества**. Схемы обмана постоянно меняются, появляются всё новые и изощренные методы, поэтому **важно регулярно обновлять знания и делиться ими с окружающими**.

2. **Установите кодовое слово в семье,** которое можно использовать для подтверждения, что человек действительно свой. Это поможет быстро распознать мошенников.

3. **Будьте внимательны при звонках и сообщениях —** всегда проверяйте, кто и зачем вам звонит, особенно если номер неизвестен. В любой непонятной ситуации кладите трубку и говорите: «Я перезвоню», а затем свяжитесь с организацией по официальному номеру телефона, чтобы уточнить, действительно ли вам звонили, например, из банка или другой службы. Никогда не перезванивайте по номеру, который вам продиктовали в сообщении или по телефону.

4. **Не разглашайте личные данные** — никогда не сообщайте номер паспорта, банковские данные, коды из SMS, пароли по телефону или в

интернете.

5. **Установите техническую защиту.**
   Поставьте определитель номера, блокировщик спама, антивирус. Это поможет отсеять подозрительные звонки и сайты еще до контакта с вами.

6. **Не торопитесь принимать решения** — мошенники часто создают ощущение срочности, чтобы заставить вас действовать быстро. Остановитесь и подумайте, проверьте информацию **в официальном источнике или обратитесь за помощью к близким родственникам**.

Что делать, если ответили на звонок мошенника:

- **Не поддавайтесь на провокации** — не обсуждайте личные данные, не подтверждайте операции и не переводите деньги.
- **Сохраняйте спокойствие** — если звонящий настойчив, просто отключите трубку.
- **Запишите номер телефона и детали разговора** — если возможно, чтобы позже сообщить в полицию или банк.
- **Сообщите о звонке в банк и правоохранительные органы** — предупредите их, чтобы они могли помочь и предотвратить дальнейшие мошенничества.
- **Проверьте состояние своих счетов и карт** — убедитесь, что нет подозрительных операций, при необходимости заблокируйте карты.

Как распознать обман:

- **Неожиданные звонки и сообщения** — особенно с просьбами перевести деньги или сообщить код из СМС.
- **Срочность и давление** — мошенники часто говорят, что время на размышления нет и нужно действовать быстро.

- **Предложения невероятно выгодных сделок или выигрышей** — если что-то звучит слишком хорошо, чтобы быть правдой, скорее всего это обман.

- **Ошибки в речи и письме** — мошенники часто используют неофициальный стиль, много ошибок или непрофессиональную лексику.

- **Подмена номеров и маскировка** — звонок может приходить с номеров, похожих на официальные, но с небольшими отличиями.

Модели поведения при звонках мошенников:

Модель поведения 1: Прекратить разговор

1. **Что происходит?**
   - Мошенник давит угрозами: «Вы обязаны…», «Если бросите трубку — ответственность» и др.
   - Он пытается удержать вас на линии, чтобы продолжить обман.

2. **Как действовать?**
   - **Прекращайте разговор при первых подозрениях, скажите:**
     — «Извините, я не могу продолжать разговор»
     — «Я должен(на) посоветоваться с близкими»
     Если вас просят остаться на линии — спокойно повторите:
     — «Я прекращаю разговор»
   - **Положите трубку.**

3. **Не верьте угрозам**
   - Мошенник может представиться сотрудником полиции, банка или Следственного комитета — это ложь.
   - Закон не предусматривает ответственности за прекращение разговора с мошенником.

4. **Если тяжело резко бросить трубку, то используйте вежливые фразы:**
   — «Извините, мне неудобно сейчас разговаривать»

— «Я перезвоню позже»

5. **Защитите свои личные границы**
    - Помните: телефон — как дверь в ваш дом.
    - Не впускайте посторонних в личное пространство, даже если кажется невежливым бросить трубку.

Модель поведения 2: Отвлечься и сохранить спокойствие

1. **Что происходит**
    - Мошенники стремятся вызвать у вас страх и панику, чтобы вы не могли рационально мыслить.
    - Часто используют много приказов и требований в повелительном наклонении.

2. **Как действовать?**
    - **Не поддавайтесь панике**

      Сделайте 3 глубоких вдоха и медленных выдоха.

      Напомните себе: «Я в безопасности, я контролирую ситуацию».
    - **Отвлекитесь на что-то физическое:**

      Понюхайте цветок или любой приятный запах.

      Посмотрите в окно или на спокойный предмет.

      Выпейте воды.
    - **Скажите:**

      — «Подождите, я сейчас вернусь к вам»

      — «Мне нужно подумать»

      — «Я перезвоню вам позже»

3. **Если давление продолжается**
    - Перейдите к модели 1 и завершите разговор.

12. Законодательные меры по борьбе с мошенничеством

Какие законы защищают граждан:

В России граждан защищают несколько ключевых законов, направленных на борьбу с мошенничеством и защиту прав потребителей. ***Виды законов и их подробное описание описаны в Приложении 4.***

Новые меры (2024-2025):

Добавлено примечание ([2]): Источник https://t.me/babikov_ab/338

- Банки обязаны «охлаждать» подозрительные операции на срок 2 дня и уведомлять об этом клиента. С июля 2024 года введено новое правило для банков: они обязаны приостанавливать подозрительные переводы на срок до 2 дней, если получатель внесён в «чёрный список» Центрального банка. Если банк нарушит это правило и не остановит подозрительный перевод, он обязан возместить клиенту причиненный ущерб в течение 30 дней.

- Запрет на иностранные мессенджеры. С 1 июня 2025 г. часть организаций больше не могут использовать иностранные мессенджеры для служебных целей. Ограничение распространяется на госорганы, компании с госучастием, банки, маркетплейсы и соцсети с аудиторией от 100 тысяч пользователей. В последние годы гражданам поступали мошеннические звонки и сообщения от лица «налоговиков», «майоров ФСБ» и «лейтенантов полиции». Часто

такие «должностные лица» звонят и пишут в WhatsApp или Telegram — так сложнее отследить их и пробить номера телефонов.

- Задержка SMS-кодов до завершения звонков. Кроме того, с 1 июня 2025 г. начал действовать новый способ защиты от мошенников - СМС-коды только после завершения звонка. Операторы связи обязаны задерживать отправку СМС с кодами подтверждения до окончания телефонного разговора. Это затруднит схемы, когда злоумышленники одновременно звонят и пытаются получить доступ к банковским операциям.

- Ограничения на передачу SIM-карт не родственникам. Согласно вступающим в силу поправкам, передавать SIM-карты, оформленные на физическое лицо, теперь разрешается только ближайшим родственникам. В их число входят родители, братья и сестры, в том числе сводные, бабушки, дедушки, дети и внуки.

- Снять самозапрет на кредиты станет сложнее. Граждане, ранее установившие самозапрет на оформление кредитов, теперь не смогут снять его просто через Госуслуги. Для отмены понадобится усиленная квалифицированная электронная подпись (УКЭП). Это сделано для защиты от мошенничества.

- Ограничения на выдачу наличных с банкоматов. Банки смогут временно ограничивать выдачу крупных сумм через банкоматы, если заподозрят, что клиент действует под давлением мошенников. Максимум – 50 000 рублей в сутки на два дня, а в месяц – не более 100 000 рублей при рисках.

- Подозрительные переводы могут быть заблокированы. Росфинмониторинг получил право приостанавливать переводы клиентов, если есть основания подозревать отмывание денег или финансирование экстремизма. Блокировки продлятся до 10 дней. Основной удар будет нанесен по организаторам схем, но ошибки не исключены. В случае ошибочной блокировки нужно обратиться в банк.

- Банки обязаны блокировать карты и онлайн-банк клиентам, которые занимаются выводом и обналичиванием похищенных денег.

- С 1 сентября 2025 года банки не смогут оформлять новые карты или подключать онлайн-банкинг тем гражданам, которые числятся в базе данных Центробанка как подозреваемые в мошеннических операциях.

13. Официальные источники информации

1. **Сайт Центрального Банка России – раздел «Противодействие мошенничеству»**
   https://www.cbr.ru/information_security/pmp/
   – Рекомендации по безопасным операциям, предупреждения о мошеннических схемах, инструкции по блокировке карт и жалобам

2. Официальные источники информации добавить **Информационный портал «Финансовая культура» Банка России**
   https://fincult.info/
   – Истории о мошенничестве, приемы защиты от мошенников

3. **Проект «Мошеловка» Народного фронта**
   moshelovka.onf.ru
   – Площадка для сообщений о мошенниках, актуальные схемы обмана, аналитика и юридические советы. Интегрируется с органами (ЦБ, МВД)

4. **Сайт МВД / Следственного комитета**
   https://tyumen.sledcom.ru/
   – Советы по безопасности, алгоритмы действий при звонках мошенников

5. **Минфин / «Стоп мошенник!»**
   https://xn--80apaohbc3aw9e.xn--p1ai/stop-moshennik/
   – Партнерский проект Минфина с правилами безопасного поведения в онлайн-среде

6. **ФЗ-152 «О персональных данных» и Гражданский кодекс РФ**
   – Официальные законодательные документы, регулирующие обработку личной информации и возмещение ущерба.

7. **Прокуратура Тюменской области**
   https://epp.genproc.gov.ru/web/proc_72

8. **УМВД по Тюменской области**
   https://72.xn--b1aew.xn--p1ai/

9. **Детская безопасность в сети. Проект Департамента информатизации Тюменской области**
   https://kiber.admtyumen.ru/
   – Образовательные материалы для детей, родителей и педагогов: как защитить ребенка в интернете, распознать риски и безопасно пользоваться цифровыми сервисами

10. **Сбер – раздел «Кибербезопасность»**
    https://www.sberbank.ru/ru/person/kibrary
    – Полезные советы по защите данных и счетов, разбор реальных схем мошенников, инструкции по безопасному использованию онлайн-сервисов

11. **Проект Правительства Тюменской области,** при поддержке Прокуратуры Тюменской области, Управления МВД России по Тюменской области и Отделения банка России по Тюменской области стопмошенники72.рф

Почему этим источникам можно доверять:

- Разработаны и поддерживаются **государственными органами**: Центральным банком, МВД, Минфином, Следственным комитетом.

- **Регулярно обновляются** с учетом новых преступных схем и технологий.

- Предоставляют **реальные инструменты для защиты**: горячие линии, шаблоны жалоб, черные списки, контроль участников.

14. Что делать, если вы стали жертвой

Если вы поняли, что стали жертвой мошенников — действуйте **немедленно**. Время имеет значение.

Шаг 1. Прекратите контакт с мошенниками

- Немедленно **завершите разговор**, **переписку**, **не отвечайте на новые сообщения**.
- Не предпринимайте никаких действий по их инструкциям.

Шаг 2. Свяжитесь с банком

- Позвоните в **службу поддержки банка**, где у вас открыт счет или карта.
- **Заблокируйте карту**, счет, онлайн-доступ — даже если перевод ещё не прошёл.
- **Напишите заявление в отделении банка** о несогласии с операцией и возьмите выписку по счету.

  С 1 октября 2025 года можно подать обращение о мошеннической операции в свой банк в его мобильном приложении (касается крупных банков). Там же будет сформирована справка по операции для предъявления в полицию.

Шаг 3. Обратитесь в полицию

- Подайте **заявление в отделении МВД**, либо **через портал Госуслуг**.
- Укажите все известные данные: телефоны, номера карт, чаты, скриншоты, ссылки.
- Вам обязаны выдать **талон-уведомление** о принятии заявления.

Контакты:

- Горячая линия МВД России: 8 495 667-74-47
- Портал подачи заявления: https://госуслуги.рф

Шаг 4. Сообщите в Роскомнадзор

Если вы передали **персональные данные** (паспорт, СНИЛС, ИНН и др.) — обратитесь в Роскомнадзор с жалобой на незаконную обработку.

Контакты:

- Сайт: https://rkn.gov.ru
- Онлайн-приемная: https://rkn.gov.ru/treatments/ask-question/
- Телефон: 8 800 550-50-99

Шаг 5. Проверьте кредитную историю

Если вы передавали паспортные данные — мошенники могли взять **кредит на ваше имя**.

Проверьте бесплатно через ЦККИ (Центральный каталог кредитных историй): https://cbr.ru/ckki/

Также можно использовать Госуслуги или бюро кредитных историй (НБКИ, Эквифакс и др.).

Шаг 6. Предупредите знакомых

- Если вы передали доступ к своим аккаунтам, почте, соцсетям — срочно смените пароли и включите **двухфакторную аутентификацию**.

- Уведомите близких, чтобы они не стали следующими жертвами от вашего имени.

Приложение 1.

Бесплатные сервисы защиты от мошенников

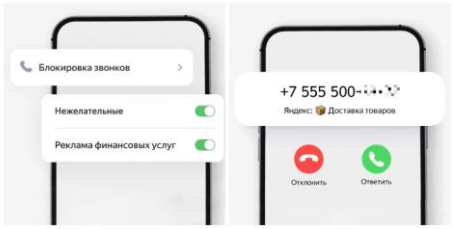
1. **Яндекс**

Добавлено примечание ([3]): https://yandex.ru/yandexapp/ru/callerid/

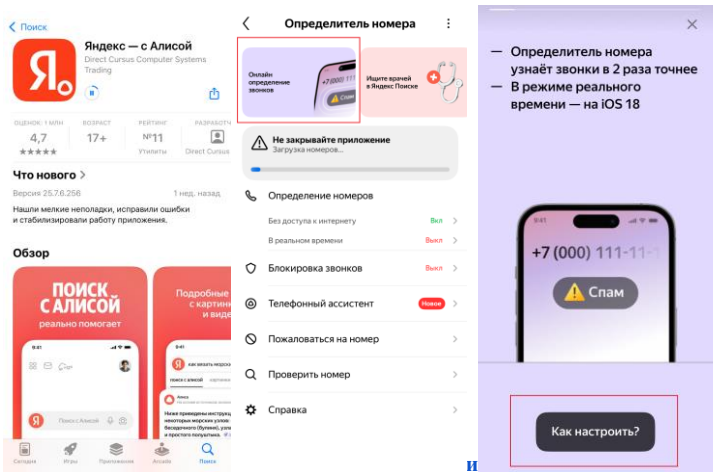
Бесплатный автоопределитель номеров работает со звонками не только по телефону, но и через WhatsApp. Сервис помечает нежелательные звонки, а также определяет категорию звонящего (медицина, банковские услуги и так далее).

База «Яндекса» собирательная: в ней данные из открытых источников, от «проверенных партнёров» и полученные на основе отзывов пользователей. Помимо идентификации номеров есть опция блокировки нежелательных звонков и рекламы финансовых услуг.

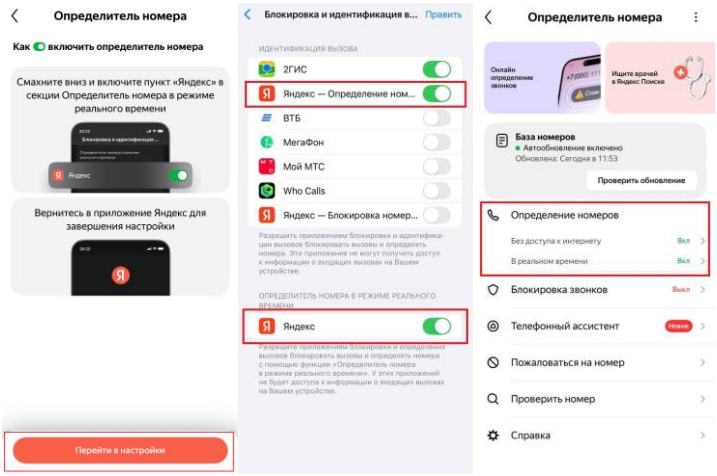
Активация: в приложении «Яндекс — с Алисой» или «Яндекс Браузер» активируйте «Алису» и попросите включить определитель номера либо нажмите на плашку «Включи АОН» (предлагается при нажатии на иконки помощника).



Установка на IOS



и

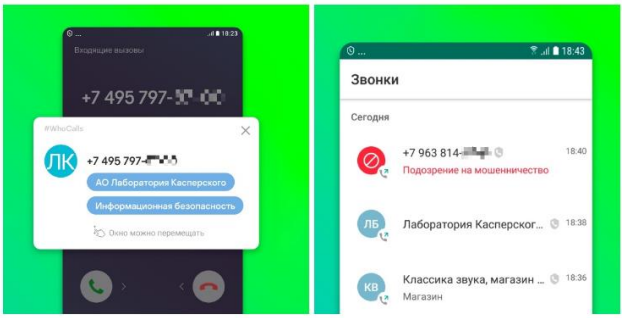


Установка на Android

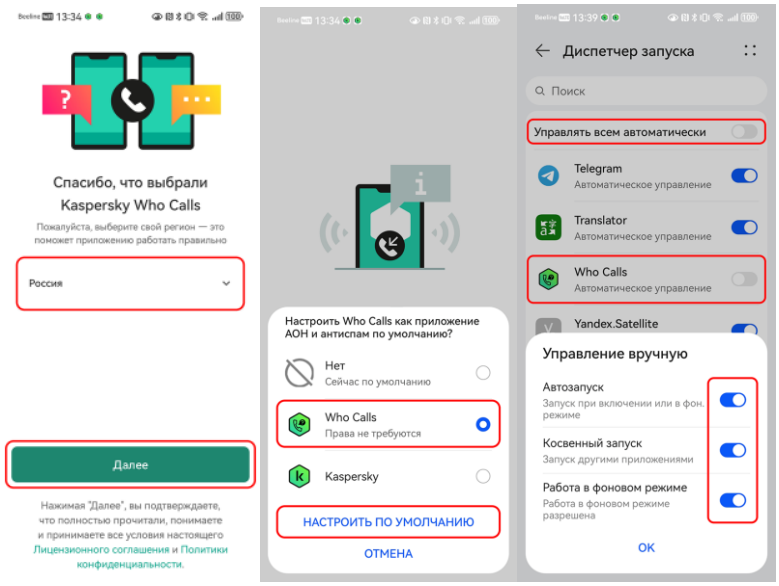
2. Kaspersky Who Calls

Определитель от «Лаборатории Касперского» сочетает базу номеров с системой на основе искусственного интеллекта для вычисления спамеров.
У этого сервиса есть премиум-подписка, из-за чего возможности бесплатной версии ограничены. В частности, она имеет рекламу и может только распознавать звонки мошенников, а также определять название и тип организации. С подпиской можно блокировать входящие звонки по категориям, использовать базу без подключения к интернету и блокировать SMS-фишинг.

Активация: загрузите приложение Kaspersky Who Calls и следуйте инструкции по настройке.

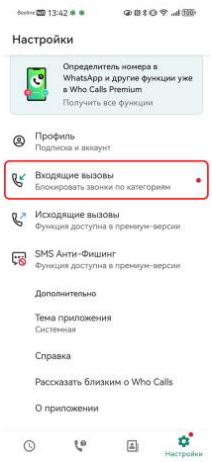


Установка на Android

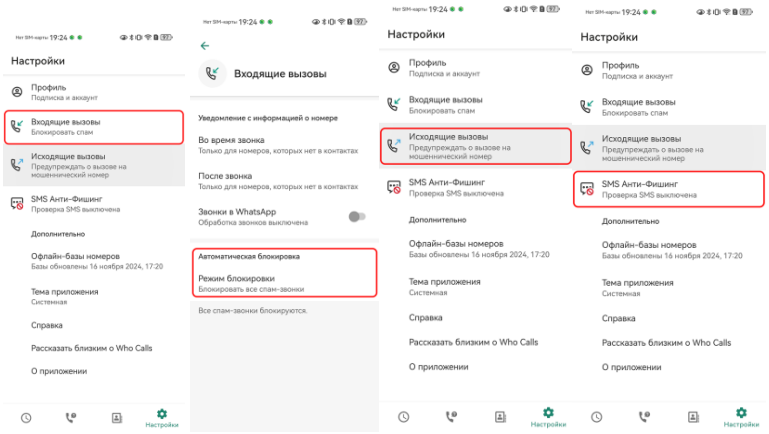


Настраиваем бесплатную версию для Android

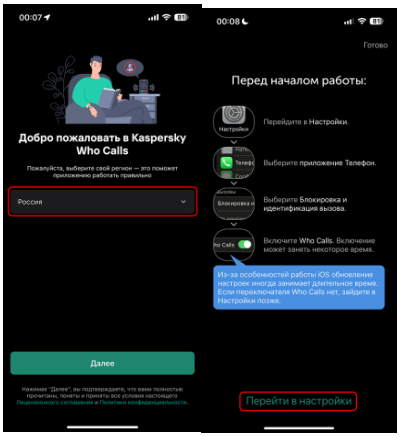
Добавлено примечание ([4]): https://www.kaspersky.ru/blog/installation-and-setup-of-kaspersky-who-calls/38547/



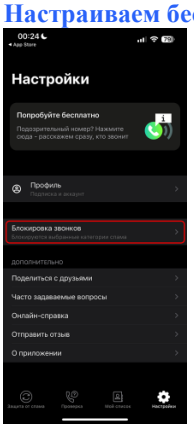
Настраиваем платную версию Kaspersky Who Calls для Android



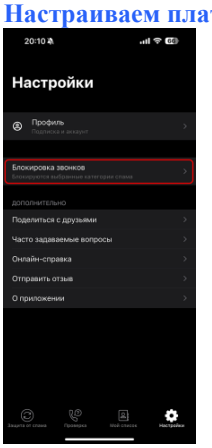
Установка на IOS



Настраиваем бесплатную версию для iOS

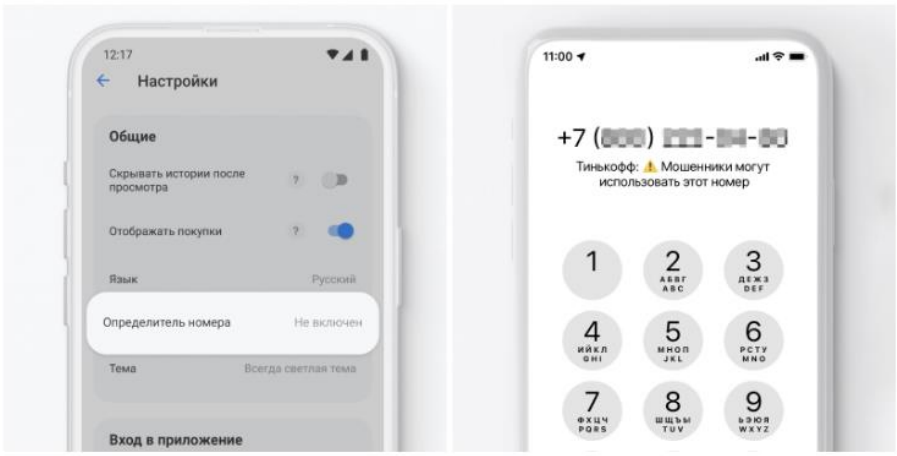


Настраиваем платную версию для iOS



3. ВКонтакте

Добавлено примечание ([5]): не могу най инструкцию

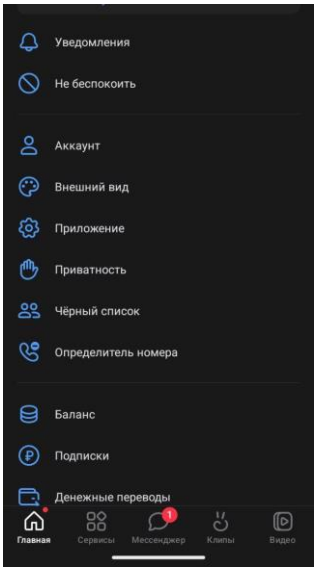


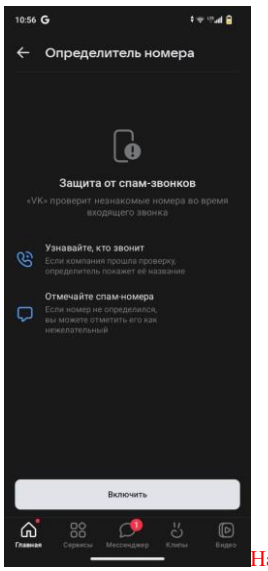
Возможности сервиса стандартные: на основе отзывов пользователей он предупреждает о нежелательных звонках, показывает название компании и сферу её деятельности. Мессенджер использует умные алгоритмы, чтобы выявлять спамеров, мошенников, коллекторов и «молчунов»: запрашивает отзыв пользователей, если заметит необычную продолжительность или частотность звонков с конкретных номеров.

База нежелательных номеров загружается на смартфон, чтобы функция работала даже без подключения к интернету. Эту базу можно обновлять в настройках функции.

Активация: в приложении нажмите «Настройки» → «Определитель номера» и выдайте разрешения на доступ к службам телефона (при необходимости). Далее выберите «ВКонтакте» службой определения номера и защитой от спама по умолчанию.

Установка на Android



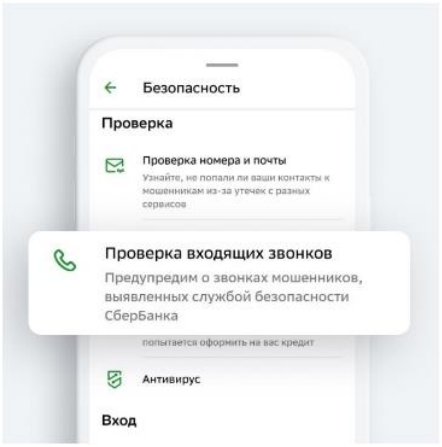


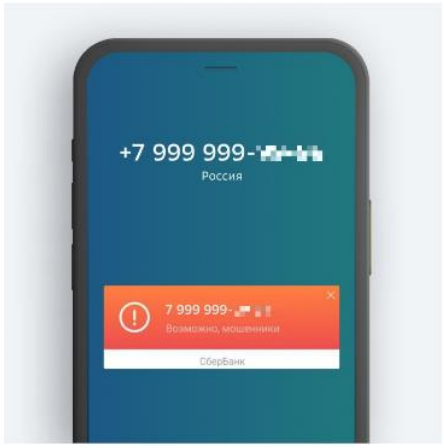
На ios не нашла пока

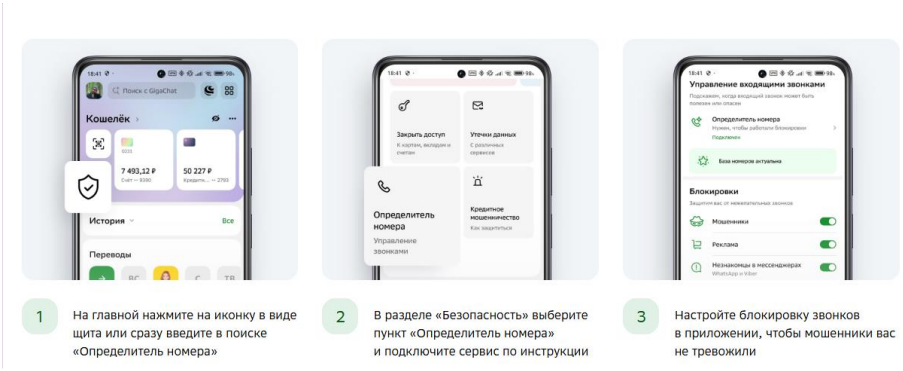
Программы от ключевых банков России

1. **Сбер / СберМобайл**

Добавлено примечание ([6]): https://www.sberbank.ru/ru/person/cybersecurity/callerid







Добавлено примечание ([7]): но у себя я такое не нашла!

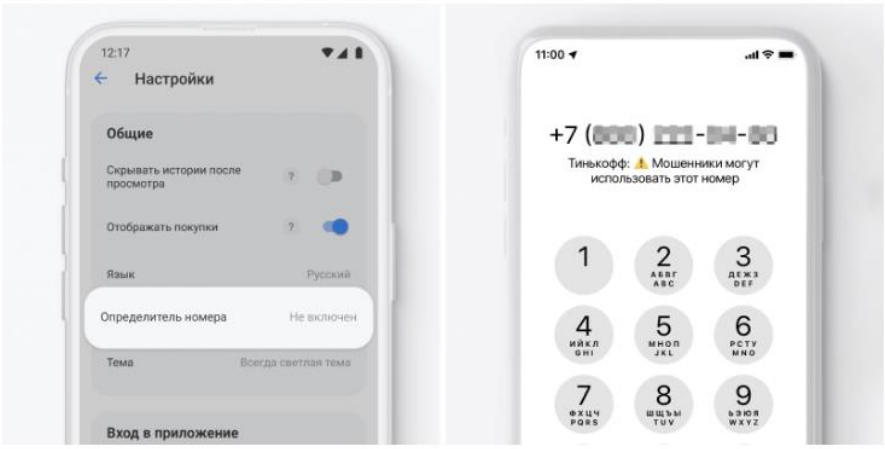
У «Сбера» определитель заточен только под выявление мошенников. Он предупредит, если кто-то жаловался на этот номер, но принадлежность к какой-либо компании или категории не отобразит. База обновляется ежедневно на основе сообщений пользователей.

На официальном сайте отмечается, что помимо базы функция опирается на особую модель от экспертов по кибербезопасности банка. Она призвана выделять потенциальных мошенников.

Активация: в приложении банка нажмите «Профиль» → «Настройки» → «Безопасность» → «Проверка входящих звонков» → «Перейти в настройки телефона». В открывшемся пункте настроек выберите «СберБанк», чтобы установить стандартной службой определения номеров и защиты от спама.

2. Т-Банк / Тинькоф Мобайл

Добавлено примечание ([8]): https://www.tbank.ru/bank/help/interfaces/bank-app/security/caller-id/



Ссылка: https://www.tbank.ru/finance/blog/save-money/

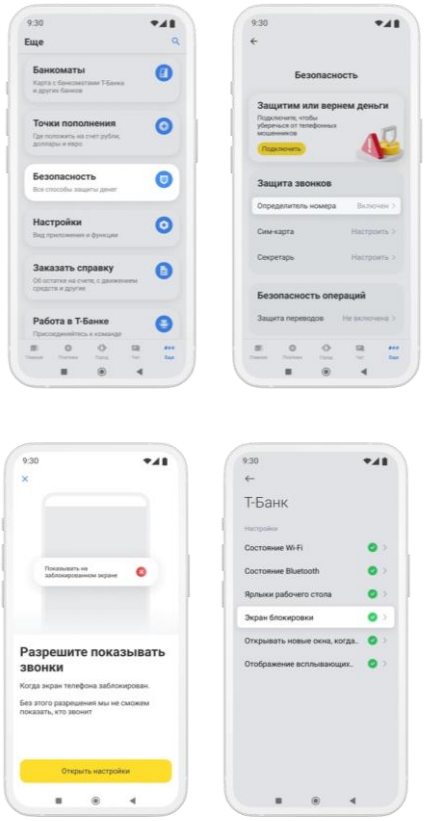
https://www.tbank.ru/mobile-operator/features/callerid/

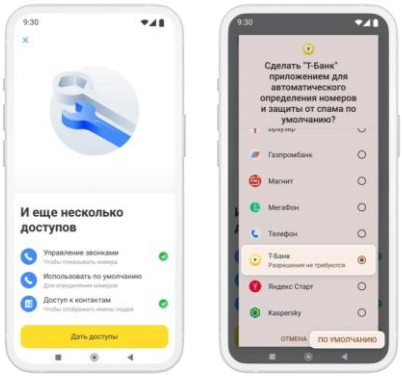
Банк предлагает услугу определения номеров всем клиентам вне зависимости от оператора связи. Функция бесплатная, база обновляется ежедневно после запуска приложения.

Звонки распределяются на три категории: проверенные номера (зелёная иконка), отвечать с осторожностью (жёлтая) и высокий риск рекламы, спама или мошенников (красная). При наличии данных звонки идентифицируются: например, как клиника, банк или доставка.

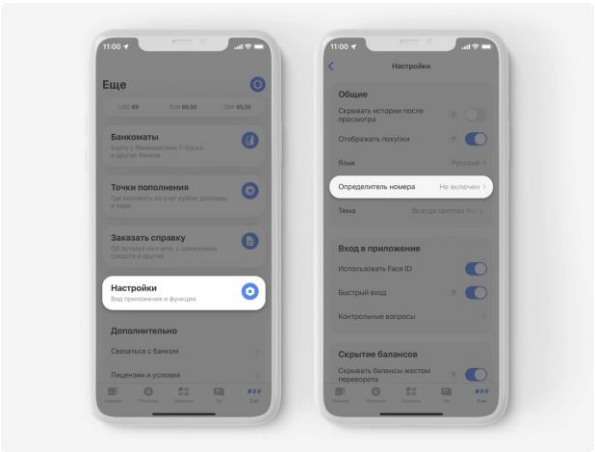
Активация: в приложении банка нажмите «Ещё» → «Настройки» → «Определитель номера» → «Продолжить» и выдайте разрешения на доступ к службам телефона (при необходимости). Далее выберите «Тинькофф» службой определения номера и защитой от спама по умолчанию.

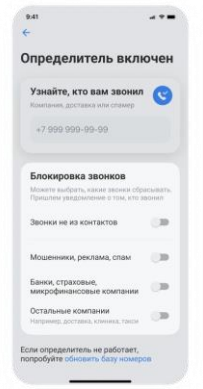
Как подключить определитель на Android

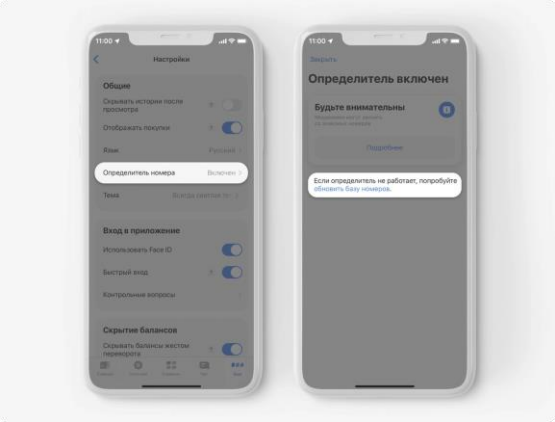




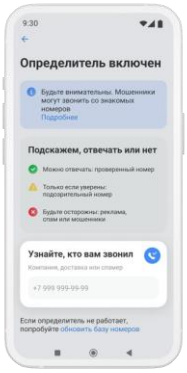
Как подключить определитель на iPhone







Как проверить номер в базе данных определителя Т-Банка



3. ВТБ Онлайн

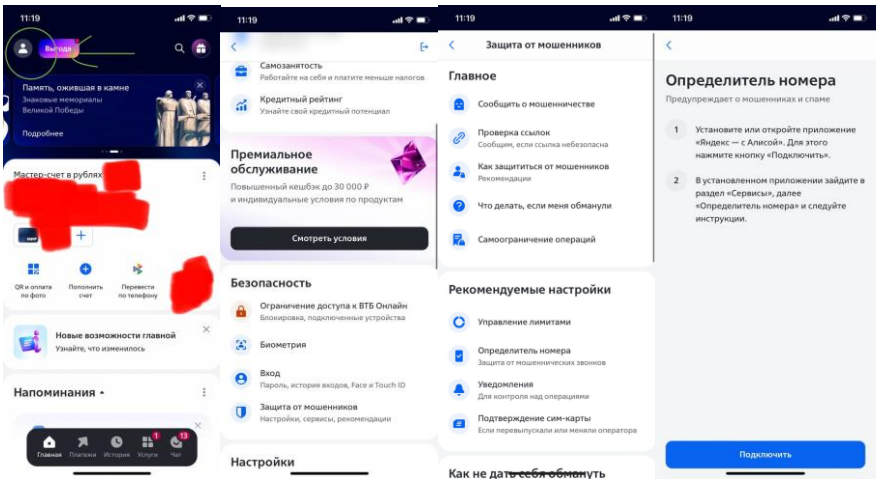
ВТБ предлагает сервис «Определитель номера», который позволит узнавать детали о входящем звонке с неизвестного номера прямо во время вызова. Функционал доступен для 8,4 млн пользователей приложения «ВТБ Онлайн» на платформе Android, указано в сообщении банка.

«Определитель номера не только покажет, от какой компании поступает звонок, но и отметит, если звонок может быть полезен. Например, «Служба доставки», «Медицинские услуги», «Вероятно, полезный звонок» и другие», — рассказали в кредитной организации.

Во время вызова в дополнение к номеру пользователь может увидеть пометку: «Подозрение на мошенничество», «Спам! Есть жалобы», «Реклама товаров и услуг», «Возможно, звонок из банка. Не сообщайте свои пароли и коды».

Подключить функцию автоматического определения номера можно бесплатно в мобильном приложении «ВТБ Онлайн» в разделе «Услуги» в одноименном блоке на платформе Android. ВТБ также адаптировал данную опцию для людей с ограничениями здоровья.

на IOS



Программы от операторов сотовой связи

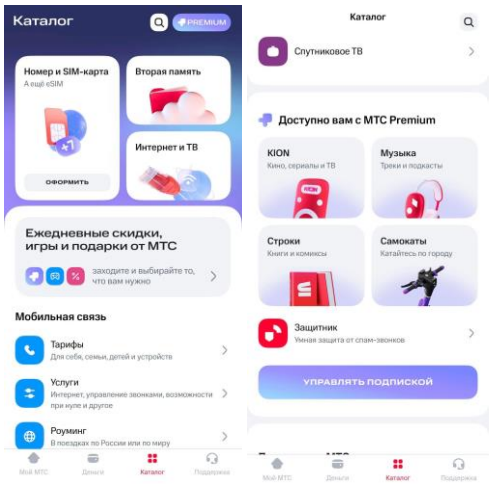
1.МТС

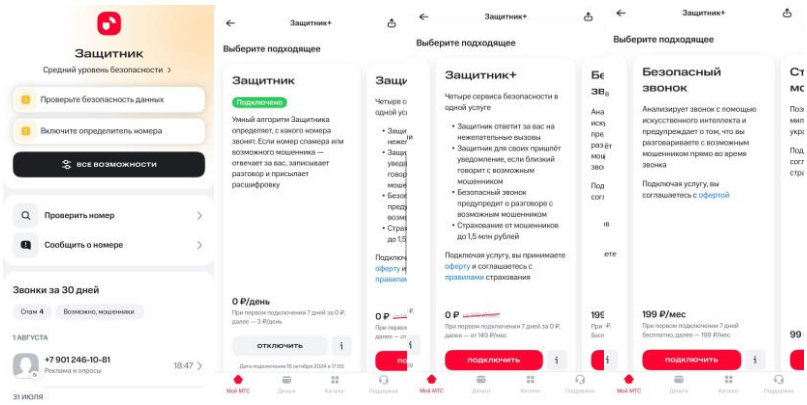
- **Услуги:**
  «Защитник» — антимошенническая услуга за 3 рубля в день, блокирует нежелательные звонки и SMS.
  «Определитель номера» — бесплатная услуга, показывает, кто звонит.
- **Как подключить:** через личный кабинет на сайте МТС или в официальном мобильном приложении → выбрать нужную услугу и активировать.
- **Как использовать:** после подключения при входящем звонке появится информация о звонящем, а нежелательные вызовы будут блокироваться автоматически.

Добавлено примечание ([9]): https://support.mts.ru/zaschitnik/opredelitel-nomera/kak-vklyuchit-opredelitel-nomera

МТС.Защитник

Услуга "МТС Защитник" предназначена для защиты абонентов МТС от мошеннических и спам-звонков. Она автоматически определяет, является ли звонок нежелательным, блокирует его и предоставляет расшифровку разговора, если это необходимо.





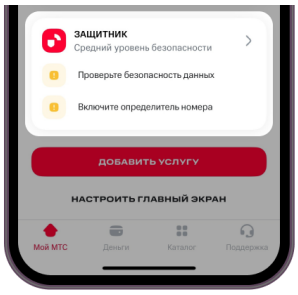
Как включить Определитель номера

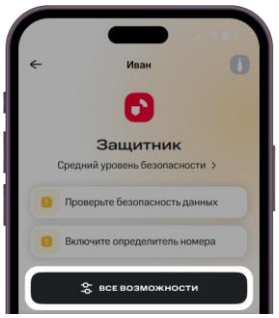
Добавлено примечание ([10]): https://support.mts.ru/zaschitnik/opredelitel-nomera/kak-vklyuchit-opredelitel-nomera

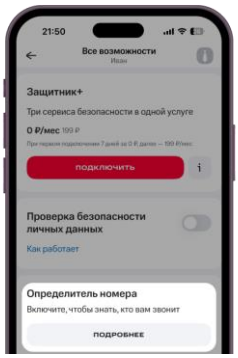
1. На главном экране приложения Мой МТС нажмите на виджет Защитник
2. Нажмите Все возможности
3. В разделе Определитель номера нажмите Подробнее
4. На открывшемся экране нажмите на кнопку:
   «К настройкам» — на айфоне
   «Включить» — на андроиде

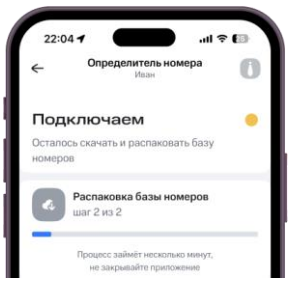
Вы перейдёте в настройки телефона. Выберите Мой МТС приложением для определения номеров. На айфоне в разделе Блокировка и идентификация вызова включите Мой МТС

5. Запустится скачивание и распаковка базы номеров. Этот процесс может быть довольно долгим. Пока он идёт, важно:
   не закрывать приложение Мой МТС
   не выходить из него
   не переводить телефон в спящий режим









2. Мегафон

- **Услуги:**
  «Знаю, кто звонит Plus» — за 3,5 руб/день, показывает информацию о звонящем.
  «Черный список» — 1 руб/день, блокирует нежелательные номера.
  Kaspersky от Мегафона — 2 руб/день, комплексная антимошенническая защита.
- **Как подключить:** через личный кабинет на сайте Мегафон или мобильное приложение → выбрать и подключить услуги.
- **Как использовать**: после активации услуги автоматически показывается информация о звонящем и включается блокировка.

3.Билайн

- **Услуги:**
  «Кто звонит» — 3 рубля в сутки, определяет номера.
  «Черный список» — блокировка нежелательных номеров.
  «Антифрод-платформа» — защита от мошеннических звонков и подменных номеров.
- **Особенность:** в услугу входит виртуальный помощник, который анализирует звонки и блокирует подменные номера.
- **Как подключить:** через приложение «Билайн» → в разделе услуг выбрать нужные функции и активировать.
- **Как использовать:** сервис работает автоматически, при входящем звонке показывает данные звонящего и блокирует спам.

4. Теле2

- **Услуги:**
  «Черный список» — блокирует нежелательные номера.
  «Антиспам» — фильтрация спам-звонков.
  «SMS-фильтр» — блокировка подозрительных SMS.
- **Как подключить**: через приложение «Мой Теле2» → выбрать нужные услуги и подключить.
- **Как использовать:** после активации услуги начинают автоматически фильтровать звонки и сообщения.

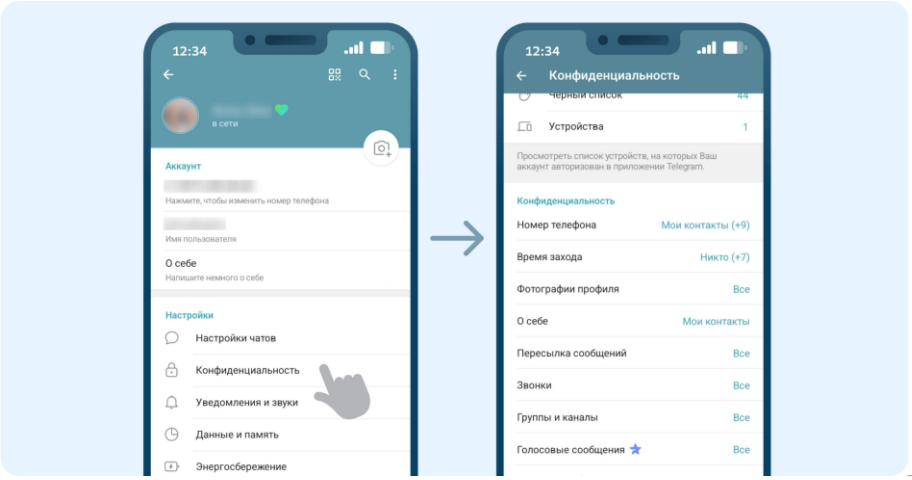
Приложение 2.

Инструкция по обеспечению безопасности мессенджеров

Инструкция для iOS

Telegram

1. Откройте Telegram
2. Нажмите на «Настройки» (внизу справа).
3. Перейдите в «Конфиденциальность» → «Звонки».
4. В разделе «Кто может звонить мне» выберите:
 - «Контакты»— звонки только от сохраненных номеров.
 - «Никто»— полный запрет (можно добавить исключения).
5. (Опционально) Нажмите «Добавить исключения», чтобы разрешить звонки от конкретных людей.



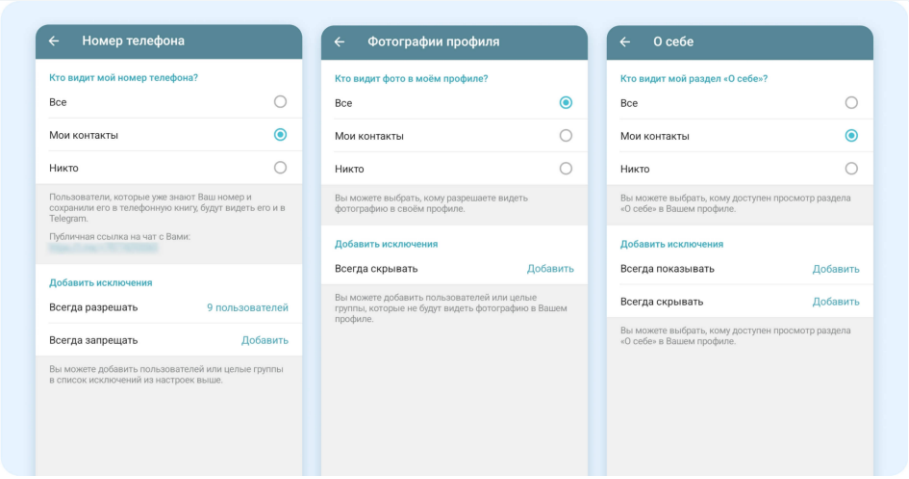
Добавлено примечание ([11]): https://www.sberbank.ru/ru/person/kibrary/reminders/kak-nastroit-konfidencialnost-v-telegram

1. Перейти в раздел «Номер телефона» и настроить отображение номера

При этом можно перейти в подраздел «Исключения» и добавить пользователей, которые будут видеть номер всегда, а также тех, кто не увидит его никогда

2. Перейти в раздел «Фотографии профиля» и настроить отображение фото

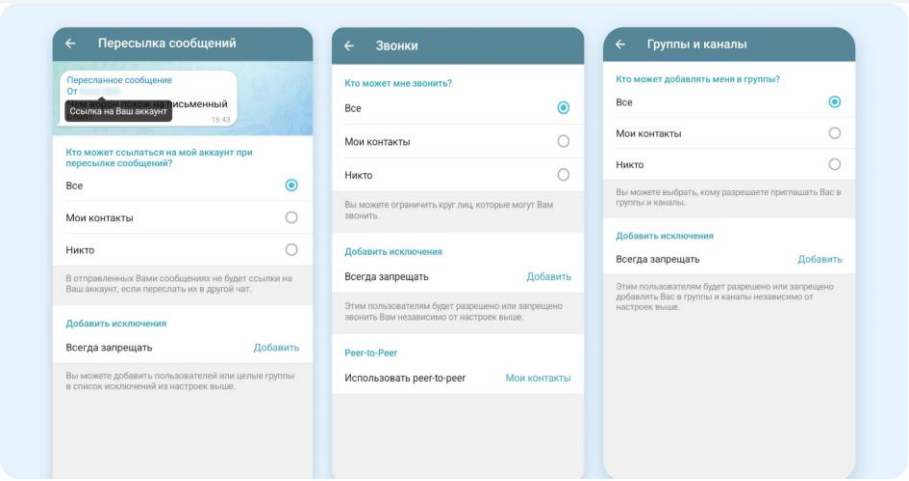
3. В разделе «О себе» можно настроить отображение данной информации



4. Перейти в раздел «Пересылка сообщения» и настроить возможность просмотра вашего профиля

5. Перейти в раздел «Звонки» и настроить возможность звонка

6. Перейти в раздел «Группы и каналы» и настроить возможность добавлять вас в группы и каналы



Для особенно осторожных

Если вы хотите, чтобы никто не смог просматривать ваш IP-адрес при звонках, то в разделе «Звонки» в подразделе «Peer-to-Peer» выберите пункт «Не использовать».
Если не хотите – выберите пункты «Все», либо «Мои контакты»

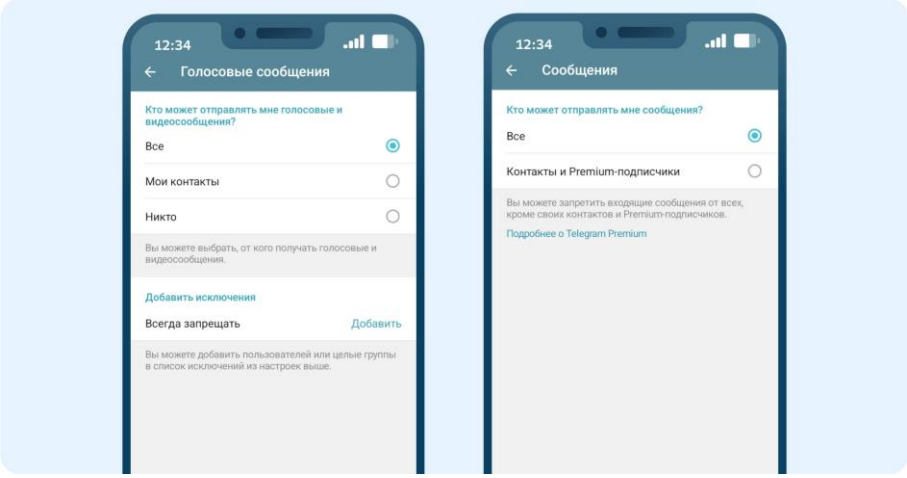
Для обладателей подписки Telegram Premium

В подписки Telegram Premium,вы можете запретить части пользователей отправлять вам сообщения и голосовые

Для этого необходимо:

1. Перейти в раздел «Сообщения» и выбрать пункт «Контакты и Premium-подписчики»

2. Перейти в раздел «Голосовые сообщения» и выбрать пункты «Мои контакты» либо «Никто»



WhatsApp

Добавлено примечание ([12]): https://faq.whatsapp.com/330710270955968/?cms_platform=iphone&helpref=platform_switcher&locale=ru_RU

1. Откройте WhatsApp
2. Перейдите в «Настройки» (вкладка справа внизу) → «Конфиденциальность».
3. Прокрутите вниз и выберите «Звонки».
4. Включите «Тихие звонки с неизвестных номеров» (ползунок станет зеленым).
   - Теперь звонки от незнакомцев будут приходить без звука, но уведомление появится в чате.

Инструкция для Android

Telegram

1. Откройте Telegram
2. Нажмите на ≡ (три полоски) в левом верхнем углу.

3. Перейдите в «Настройки» → «Конфиденциальность».

4. Выберите «Звонки».

5. В разделе «Кто может звонить мне» выберите:

- «Контакты»— звонки только от сохраненных номеров.
- «Никто»— полный запрет (можно добавить исключения).

6. (Опционально) Нажмите «Добавить исключения», чтобы разрешить звонки от конкретных людей.

WhatsApp

1. Откройте WhatsApp

2. Нажмите на ⋮ (три точки) в правом верхнем углу.

3. Перейдите в «Настройки» → «Конфиденциальность».

4. Прокрутите вниз и выберите «Звонки».

5. Включите «Тихие звонки с неизвестных номеров» (ползунок станет зеленым).

- Теперь звонки от незнакомцев будут приходить без звука, но уведомление появится в чате.

Приложение 3.

Инструкция по обеспечению безопасности компьютера

ШАГ 1. Не переходите по сомнительным ссылкам

Как определить, что ссылка сомнительная?

- Адрес выглядит подозрительно: содержит набор символов, лишние точки, подмену букв (например, g0suslugi.ru).
- Использует сокращатели ссылок (bit.ly, goo.gl) без пояснения.
- Ссылка пришла от незнакомого отправителя или в странном сообщении.
- Вызывает чувство спешки или страха: «Срок оплаты истекает сегодня», «Вас оштрафуют» и т. д.

Что делать, если вы получили сомнительную ссылку

- Не нажимайте и не открывайте ее.
- Проверьте ссылку через сервисы вроде Google Safe Browsing.
- Если ссылка пришла от «знакомого» — свяжитесь с ним другим способом и уточните.
- Сообщите в службу безопасности (работодатель, IT-отдел) при необходимости.

Как безопасно работать с ссылками

- Никогда не кликайте по ссылке, если не уверены на 100%.
- Используйте расширения браузера, предупреждающие об опасных сайтах.
- Отключите автоматическое открытие ссылок в мессенджерах и почтовиках.

Видите ссылку? Задайте себе вопросы:

1. *Адрес выглядит подозрительно?*
   (много символов, ошибки, странное доменное имя)
   → **Да** → Не открывайте ссылку.
   → **Нет** → Перейдите к следующему вопросу.
2. *Сообщение с ссылкой акцентирует внимание на срочности и вызывает тревогу?*
   (например: «оплатите срочно», «вы нарушили закон»)
   → **Да** → Не открывайте.
   → **Нет** → Следующий вопрос.
3. *Ссылка использует сокращенный адрес (bit.ly, goo.gl и т.п.)?*
   → **Да** → Проверьте ссылку через сервисы проверки (CheckShortURL, Unshorten.It)
   → **Нет** → Следующий вопрос.
4. *Вы уверены, что отправитель — это знакомый человек или организация?*
   → **Нет** → Не открывайте. Свяжитесь с отправителем другим способом.
   → **Да** → Можете перейти по ссылке, но с осторожностью

ШАГ 2. Не подключайте чужие USB-накопители

Почему это опасно

- Устройство может содержать автозагрузку вируса, запускаемого сразу при подключении.

Как определить, можно ли доверять флешке

- Убедитесь, что устройство принадлежит проверенному человеку.
- Просканируйте накопитель антивирусом до открытия файлов.

Альтернатива

- Для обмена файлами используйте облачные сервисы с проверкой доступа (Google Drive, Dropbox).

Получили флешку? Задайте себе вопросы:

1. *Вы точно знаете, кому она принадлежит?*
   → **Нет** → Не подключайте
   → **Да** → Следующий вопрос
2. *Вы проверили ее антивирусом до открытия файлов?*
   → **Нет** → Выполните полное сканирование
   → **Да** → Следующий вопрос
3. *Использовалась ли флешка в подозрительных местах (интернет-кафе, чужие персональные компьютеры)?*
   → **Да** → Лучше не использовать
   → **Нет** → Можно работать с осторожностью

ШАГ 3. Не скачивайте фальшивое антивирусное ПО

1. Как распознать фальшивый антивирус

- Приходит из спам-писем или всплывающих окон.
- Имитирует официальный интерфейс, но требует немедленной установки.

2. Где скачивать официальные приложения

- Только с официальных сайтов: kaspersky.ru и др.
- Через встроенные магазины приложений (Google play, Apple App Store).

3. Что делать, если вы уже скачали подозрительное приложение

- Не запускайте его.
- Удалите файл, очистите корзину.
- Запустите проверку антивирусом.

Нужно установить антивирус? Задайте себе вопросы:

1. *Скачиваете с официального сайта (kaspersky.ru)?*
   → **Нет** → Остановитесь. Найдите официальный источник
   → **Да** → Следующий вопрос
2. *Установка началась после всплывающего окна или спам-письма?*
   → **Да** → Немедленно остановите процесс
   → **Нет** → Далее
3. *ПО требует срочной установки под угрозой заражения?*
   → **Да** → Не доверяйте — это подделка
   → **Нет** → Далее
4. *Проверяли ли вы это ПО по отзывам на профильных форумах или в СМИ?*
   → **Нет** → Рекомендуется провести проверку
   → **Да** → Установка допустима

ШАГ 4. Защитите веб-камеру

Как понять, что веб-камера взломана?

- LED-индикатор камеры включается без вашего действия.
- Установлено неизвестное ПО, использующее камеру.

Как защитить себя?

- Заклейте объектив непрозрачной пленкой.
- Отключите камеру в настройках BIOS или «Диспетчере устройств».

Установите антивирус с функцией защиты веб-камеры

- Например, Kaspersky Internet Security или Bitdefender.

Обратите внимание на поведение камеры:

1. *Световой индикатор загорается сам?*
   → **Да** → Отключите камеру. Проверьте запущенные процессы
   → **Нет** → Следующий вопрос
2. *Установлено ли ПО, использующее камеру?*
   → **Да** → Проверьте, легально ли оно
   → **Нет** → Далее
3. *Камера физически заклеена?*
   → **Нет** → Рекомендуется заклеить непрозрачной лентой
   → **Да** → Следующий шаг
4. *Установлен антивирус с защитой веб-камеры (Kaspersky, Bitdefender)?*
   → **Нет** → Установите современный антивирус
   → **Да** → Все хорошо, оставайтесь на контроле

ШАГ 5. Не используйте один и тот же пароль

Почему это опасно

- Один скомпрометированный аккаунт открывает доступ ко всем.

Как создать уникальные пароли?

- Используйте генераторы паролей или менеджеры (Bitwarden, LastPass).

Как управлять десятками паролей?

- Храните их в защищенных хранилищах с двухфакторной аутентификацией.

Проверьте себя:

1. *Вы используете один пароль на нескольких сайтах?*
   → **Да** → Срочно смените пароли, они уязвимы
2. *Пароли хранятся с двухфакторной аутентификацией (2FA)?*
   → **Нет** → Включите 2FA через почту, приложение или смс
   → **Да** → Отлично
3. *Регулярно обновляете пароли?*
   → **Нет** → Установите напоминание на смену каждые 3–6 мес.
   → **Да** → Продолжайте

ШАГ 6. Создавайте надежные пароли

Какой должен быть пароль

- Длина от 10 символов.
- Комбинация: заглавные, строчные, цифры и символы.

Чего избегать

- Простых комбинаций (qwerty123, password, ваша дата рождения).
- Повторяющихся символов (aaaa1111).

Проверка безопасности пароля

- Используйте сайты вроде haveibeenpwned.com, чтобы проверить утечки.

Проверьте себя:

1. *Пароль длиннее 10 символов?*
   → **Нет** → Увеличьте длину
   → **Да** → Следующий вопрос

2. *Содержит заглавные, строчные, цифры и символы?*
   → **Нет** → Сделайте его сложнее
   → **Да** → Следующий вопрос
3. *Пароль содержит простые фразы (123456, qwerty, ваша дата рождения)?*
   → **Нет** → Следующий вопрос
   → **Да** → Замените
4. *Проверяли ли вы пароль на утечки?*
   → **Нет** → Используйте:
   — https://haveibeenpwned.com
   — https://passwords.google.com
   → **Да** → Все в порядке

ШАГ 7. Обновляйте программное обеспечение своевременно

Почему это важно

- Обновления закрывают уязвимости, которые могут использовать хакеры.

Что именно нужно обновлять

- Операционную систему
- Браузеры.
- Антивирус.
- Программы с доступом к интернету.

Как это автоматизировать

- Включите автообновления в настройках.

Проверьте себя:

1. *Вы давно устанавливали обновления Windows/macOS/Linux?*
   → Да → Зайдите в настройки → Центр обновлений → Проверьте и установите
   → Нет → Отлично
2. *Ваш браузер обновляется автоматически?*
   → Нет → Проверьте вручную (Chrome: «О браузере Google Chrome»)
   → Да → Все хорошо
3. *Установлены обновления антивируса?*
   → Нет → Запустите обновление баз вручную
   → Да → Хорошо
4. *Используете программы с интернет-доступом (Zoom, Telegram)?*
   → Да → Убедитесь, что включены автообновления
   → Нет → Следующий пункт
5. *Автообновления включены в системе?*
   → Нет → Рекомендуется:
   — Windows: Пуск → Обновления и безопасность → Включить
   — macOS: Системные настройки → Обновления
   → Да → Отлично, вы защищены

ШАГ 8. Не отвечайте на фишинговые письма

Как выглядит фишинг

- Обещание выигрыша или угрозы штрафов.
- Ссылка ведет на сайт, копирующий известный бренд.

Что делать при подозрении на фишинг

- Не открывайте вложения и ссылки.
- Сверьте адрес отправителя (не только имя!).

Как повысить защиту

- Настройте спам-фильтр в почтовике.
- Включите двухфакторную авторизацию в email-сервисе.

Пришло подозрительное письмо? Задайте себе вопросы:

1. *Письмо обещает приз, угрожает штрафами, требует действий?*
   → **Да** → Скорее всего, фишинг. Не взаимодействуйте
   → **Нет** → Следующий вопрос
2. *Ссылка в письме ведет на странный или копирующий сайт?*
   → **Да** → Не переходите, проверьте URL (например, через VirusTotal)
   → **Нет** → Можно перейти, но с осторожностью
3. *Имя отправителя знакомо, но адрес подозрителен?*
   → **Да** → Это подделка. Удалите
   → **Нет** → Далее
4. *Вы случайно кликнули?*
   → **Да** → Немедленно закройте страницу. Очистите кеш, проведите антивирусную проверку
   → **Нет** → Отлично
5. *Спам-фильтр в почте включен?*
   → **Нет** → Активируйте в настройках (например, «Фильтры и блокировка»)
   → **Да** → Следующий вопрос
6. *Двухфакторная защита email включена?*
   → **Нет** → Включите через настройки безопасности
   → **Да** → Безопасность усилена